Protecting The Vulnerable: Dimensions of Assisted Digital Access

LIZZIE COLES-KEMP, Royal Holloway University of London, UK
NICK ROBINSON, Royal Holloway University of London, UK
CLAUDE P.R. HEATH, Royal Holloway University of London, UK

A successful digital society is, in part, predicated on people having secure access to digitally-delivered services when they need it. It has long been recognised that parts of society are not able to access digital services without assistance, often as a result of economic precarity. During the COVID-19 pandemic, the importance of third and voluntary sector organisations in providing assisted digital access has come to the fore. As access to essential everyday services moved to digital-only and family and friendship networks of support became disrupted by the pandemic, for many, voluntary and third sector organisations were the source of digital assistance to claim welfare, pay bills, take part in education and purchase food. Our study explores the types of assisted digital access that voluntary and third sector organisations have provided thus far during the COVID-19 pandemic. We capture the dimensions of this assistance and evaluate the steps such organisations take to ensure that this access is safe for both the assister and assisted. From these findings we set out a security strategy with supporting design principles that combines digital security with human security in a security approach we term 'positive-first'.

CCS Concepts: • **Security and privacy** → *Social aspects of security and privacy*; • **Human-centered computing** → *User studies.*

Additional Key Words and Phrases: assisted access, digital divide and voluntary and third sector support

ACM Reference Format:
Lizzie Coles-Kemp, Nick Robinson, and Claude P.R. Heath. 2022. Protecting The Vulnerable: Dimensions of Assisted Digital Access. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 534 (November 2022), 26 pages. https://doi.org/10.1145/3555647

1 INTRODUCTION

Assisted digital access is a co-operative practice where an individual is assisted by another individual to access and realise the benefits of a digital service. COVID-19 and the resulting expedited transition to digital service provision for the majority of essential everyday services has not only emphasised the importance of technology being accessible for all, but also the importance of that access being safe and secure for all. During the pandemic, all age groups across many countries have seen an increase in the need to access essential services online [3] and this has challenged how we support assisted access at scale. As a result, countries such as the UK have seen a rise in people creating social networks and drawing on in-person support from voluntary and third sector organisations to access services [34]. Despite this, service providers responsible for the delivery of everyday services have been slow to formally recognise voluntary and third sector organisations as legitimate providers of digital access assistance. This has resulted in voluntary and third sector organisations

Authors' addresses: Lizzie Coles-Kemp, lizzie.coles-kemp@rhul.ac.uk, Royal Holloway University of London, Egham, UK; Nick Robinson, Royal Holloway University of London, Egham, UK; Claude P.R. Heath, Royal Holloway University of London, Egham, UK.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
© 2022 Copyright held by the owner/author(s).
2573-0142/2022/11-ART534
https://doi.org/10.1145/3555647

having to work against (rather than with) the security of digital services in order to protect those who have been made particularly vulnerable by the social and economic impacts of COVID-19.

In this paper, we present a study that responds to questions common within the CSCW domain [72] to explore the practices related to assisted digital access from the perspective of voluntary and third sector organisations, and consider what such practices might mean for the design of digital services essential for day-to-day living. We ask the following questions:

- What are the characteristics of secure assisted digital access?
- What factors shape these characteristics?
- How might digitally-delivered essential services be better designed to safely support assisted digital access?

We ground our work in a literature review, then present a qualitative study with voluntary and third sector organisations, and close with a discussion about the dimensions of assisted digital access and presentation of related design principles.

2 BACKGROUND LITERATURE

Assisted access is typically studied against the backdrop of the digital divide [18, 59, 73]. The focus of research on the digital divide has evolved from a study of simply the divide between those who do and do not have physical access to technology, into a study that includes considers the quality of access [12] and how the quality of access can be improved for all in a digitally-mediated society [32, 35, 36]. For many scholars, the quality of access relates to the use people can make of access to technology and the benefits that technology access yields [59], enabling the formation and development of different types of capital, including social and economic capital. It has been argued that digital capital is a capital in its own right and is a multidimensional concept that is composed of the material resources that enable access to digital technology and services, as well as the attitudes, abilities and capabilities that enable access more broadly [60]. However, digital capital is not only a bridging component that enables other forms of capital to be built [12, 60], but also depends on other forms of capital for itself to be built. For example, whilst economic capital is the fundamental building block by which individuals transform from a "digital have not" to a "digital have", social, cultural and political forms of capital are fundamental in shaping digital access [12, 73]. At the same time, digital capital is increasingly necessary for economic, social, cultural and political capital to be built [66]. Across all these arguments, there is an implicit assumption that access is safe and secure and that individuals are not made vulnerable by the form of access that they use.

COVID-19 brought to the fore issues related to digital exclusion [66]. In particular, access to essential everyday services such as welfare, healthcare, housing, food and education became a primary concern and highlighted the dependency many had on assistance to enable access and use of such services [61]. Economic cost, lack of digital skills and fear of online harms are all cited as reasons for digital exclusion during successive COVID-19 lockdowns in the UK [30]. In response to this, new technologies are becoming available to support safe assisted digital access. For example, a number of UK-based digital identity management platforms have built solutions that aim to support assisted access in various contexts, such as Nettoken and Trust Elevate's password and verification management tools aimed at children and digital parenting, whilst CDD Services have considered how their technologies might support notions of vouching and managing different levels of access for migrant and veteran communities across the UK. However, such technologies do not work for all assistance scenarios [3, 17]. In particular, they do not address situations where people are excluded due to a lack of social and economic capital needed to initially facilitate access, and thus build the necessary levels of trust and confidence in both the technology and the institutions delivering the services. Voluntary and third sector organisations have found themselves stepping into this gap

and delivering complex sociotechnical services in order to respond to the acute need for assisted digital access.

To understand safer assisted digital access, we summarise the main themes found in the academic literature with regard to i) assisted access, and ii) inclusive and accessible security. We then locate this synthesised body of work in the relevant literature that relates to the provision of services by voluntary and third sector organisations.

2.1 Assisted Digital Access

The phenomena of assisted digital access requires an understanding of micro-level interactions between technology and inequality, and the macro-level inequalities that are brought about by wider technology use [5]. HCI and CSCW scholarship has played an important role in developing an understanding of assisted access in relation to micro-level interactions, especially in the context of wider macro-level inequalities. This scholarship has extended the sociological understanding of assistance by taking a close look at the interaction between assistance and technological design. It has also fostered and supported studies in novel assistive technology that seeks to make technology and service access available to all.

Assisted access was first identified and discussed in sociological studies of digital access [18]. Sociological studies of digital access have long argued that access and use of technology are not monolithic concepts but are nuanced patterns of practice and interaction between people and technology in day-to-day life [74]. Shaping and supporting these interactions are networks of support from a mixture of formal and informal experts that make up what is sometimes termed as the "social envelope" around computer use [74]. Gender, age and social roles can shape the use and influence the non-use of digital technologies [74], whilst household relationships and dynamics also play a central role in forming digital access [74]. As the concept of the 'digital divide' became nuanced into a gradation of digital inclusion in the early 2000s [23], social networks that were designed to support access were identified as an important means of securing meaningful digital access. Use-by-proxy then emerged as a means by which more formalised digital access and use could take place [74]. Selwyn et al. have noted that requesting assisted access has many subtleties and can be an act of resistance, as well as a request for help, and therefore does not solely arise from a lack of capability and resource [74].

In a sociological body of work, assisted access has been framed as a composite of an individual's social and digital capital. An individual's social capital is partly composed of access to networks of people with technological knowledge who can offer the individual support [73] and digital capital that combines material access to technology with technical capabilities and know-how [60]. Sociological studies of assisted access point to support networks being heterogeneous and composed of support from multiple sources [18]. Studies have also shown that support is most likely to be socially-embedded, resulting in access to assistance being socially and culturally shaped. Notably, people receiving support in domestic settings have less access to skilled support, whereas those who have access to help in non-domestic settings - such as a work environment - have access to more skilled support [18].

HCI makes an important contribution to the study of assisted access, focusing closely on the interaction between technology design and the capabilities of technology and service users. Within HCI, research on assisted access has often focused on the particular context of access to digital financial services, and the way in which access is shared and often situated within the relations that we have with others [2]. For example, in a recent study, Barros Pena et al. consider the intersection between mental health and digital access, demonstrating how the experience of access to digital services can be shaped by mental health [7]. This work augments sociological studies by reviewing how people access services with very different pressures and emotional responses – all of which

impact on how people access systems and are able to benefit from that access. CSCW research also brings patterns of cooperation and relational services into the assisted access discussion [35, 36, 79], highlighting the importance of embedded support and the variety of ways in which support might be provided.

HCI and CSCW research in this area also reflects the relevance of economic capital for digital access, making powerful arguments for the importance of paying close attention to the social and political infrastructure that is placed around technology rollout to marginalised and underserved groups. Tawanna Dillahunt, for example, has conducted extensive research with economically marginalised groups (and ex-offenders in particular) in the U.S. as they seek support whilst job seeking [22, 56, 83]. HCI and CSCW research has further extended our understanding of assisted access by nurturing thought leadership in the area of assisted technology design. Traditionally, work at the intersection of accessibility and HCI has focused on the design and deployment of assistive technologies for people with disabilities [48]. As Kameswaran and Muralidhar [42] note, however, we have also seen a body of work emerging around *social accessibility* - which *"examines the situated use of assistive and mainstream technologies by people with disabilities, as well as the social concerns of its users"* - with studies focusing on the use and (in)accessibility of certain technologies, platforms and services, particularly for individuals with visual impairments [10, 13, 31] and other forms of physical and cognitive disabilities [8, 46, 75]. HCI scholars have added to sociological understandings of assisted access by reflecting on how technological/design interventions can be used as part of the assistance. For example, a form of digital *delegation* that can be used by a (potentially vulnerable) user, allowing a designated "helper" to conduct digital payments on their behalf [25]. Recognising some of the challenges faced by the elderly regarding the everyday use and maintenance of their personal finances - and how workarounds are often found in order to allow trusted individuals to conduct financial payments on their behalf - Dunphy et al. propose a theoretical design of a '*Helper Card*' that can be used "spontaneously and securely" by someone other than the holder of the account (and configured to give limited access to its functionality) [25]. Similarly, Barros Pena et al. demonstrate how a new API might be used to enable a third party (termed "ally") to assist with an individual with access to digital financial services [6]. Whilst both studies highlight the limitations of existing formal approaches to enabling either a trusted *helper* or third-party to assist with an individual accessing their digital financial services, we are also reminded of the workarounds that are often created that *"represent a trade-off between trust, convenience and immunization against financial abuse"* [25].

2.2 Usable, Accessible and Inclusive Security

Whilst the literature on assisted access has not typically paid close, explicit attention to matters of safety and security, there has been an uptick in people-centered design studies including security themes. In social and political theory, security can be conceptualised as both positive and negative [29, 67] where security is not only protection from harms (termed in certain traditions of security theory as negative security) but also the ability to live free from the fear of those harms taking place (termed in certain traditions of security theory as positive security). Positive security is typically included in the conceptualisation of human security [24], whereas e-safety and digital protections are typically framed as a negative form of security that offers protection from harms. In an everyday sense, security is almost invariably experienced and practised as a blend of positive and negative security [67]. A response to a security concern will usually foreground either protection or enablement. Whilst the literature that we outline in this section does indeed consider the usability, inclusivity and accessibility of security technologies, it should be noted that the focus is on protective forms of security, with an emphasis on making protection from cyber harms a more inclusive experience.

In the last five years, there has been increased focus on accessible and inclusive security [80], with work in this area bringing the focus onto trust, social relations and the usability and accessibility of security technologies. Scholars elsewhere consider how financial insecurity, and limited access to technology and the internet, evolve digital security and privacy practices in the context homeless communities [37, 65, 77] where trust networks are in short supply. In these scenarios, additional personal protection practices need to be deployed to make digital access safe and secure for the individual. The usable, accessible and inclusive security literature reflects these tensions. At the same time, in the security practice arena there has been a growing focus on societal uses of security technology. Guidance has been published for small organisations [51] and charities [49] as well as individuals. At the beginning of the COVID-19 pandemic, the UK's National Cyber Security Centre (NCSC) produced advice that covers the basic steps to staying secure online [50]. This advice focuses on the protection of devices, services and personal information. Much of this practice guidance reflects the canon of academic literature related to the design of usable, accessible and inclusive security technology. We set out some of this literature in the paragraphs below.

Usability. Inclusive and accessible security technology design has its roots in the study and practice of usable security. From the mid-1990s, usable security became part of the wider study and practice of user-centred security, and built on the foundations of early computer security thinking [69]. In 1996, Zurko and Simon introduced the term user-centred security [84], and in 1999 Adams and Sasse published their seminal paper *Users are Not the Enemy* [1], drawing attention to the ways in which poor design of security technology resulted in people making choices that left both them and their information vulnerable. Such work made HCI an important site of usable security scholarship. Fundamental to assisted access is the importance of designing usable authentication and access control systems. As a result, HCI scholars have often focused heavily on access control in the home [27, 39, 44, 45, 45] and the usability of passwords and password sharing [19, 26, 38, 38, 76]. In 2013, usability scholar Angela Sasse called for a fundamental re-imagining of user authentication as a usable activity [70]. Sasse's road map shifts us towards implicit authentication based on data collected about an individual's use of a system as a means of authentication. Publishing in 2013, Sasse observes that the burden of authentication sits with the individual rather than with the system, noting how this creates friction between an individual and the wider security mechanisms. Sasse's work also points to how it is not only the design of authentication processes and technologies within systems that are the problem. Around the same time, Bonneau and Preibusch demonstrated that part of the usability issue was also related to the lack of consistency in authentication advice given across services, as well as within individual services [9]. Such work reminds us that usability alone is not enough to provide secure digital access, and that the accessibility of the technology also needs to be explicitly considered.

Accessibility. Karen Renaud, a HCI scholar, refers to accessibility as the next frontier in human-centred cyber security [63], arguing that the usability of security technologies does not equate to accessibility, with the latter being of most importance to security research. Renaud's work offers a call to action to improve the accessibility of security controls, demonstrating that passwords, the front line of many forms of digital service access control, are inaccessible for many with reduced capacity - such as those with vision and hearing impairments, and for those with learning disabilities or with mental health issues [63, 64].

Other authentication mechanisms, in addition to passwords, are also evaluated in this literature. For example, Fanelle et al. evaluate 4 designs of audio CAPTCHAs [28]. The audience for this form of CAPTCHA is people with visual impairments. Fanelle et al. demonstrate that to make a technology both accessible and usable is challenging. Davidson et al. have also examined an alternative audible CAPTCHA, evaluating it for its vulnerability to audio recognition tools and

make recommendations for improving their resistance to such attacks [21]. Whilst such work is often intended to enable wider numbers of people to securely and independently access technology and services, digital access often still requires the involvement of a third party, such as a carer or health worker. For example, in Jiang's work on security in digital healthcare systems for those with mental health issues, co-operation with a third party was identified as one of the access strategies [40].

Inclusivity. Accessible security is part of a wider set of inclusive security considerations that not only addresses the immediate digital divide but also considers the 'second divide' [81], which includes issues such as socioeconomics, precarity and power relations that act as barriers to access [62]. For example, Briggs and Thomas consider how the set-up and use of digital identity intersects with socioeconomics [11]. In a further example, Nicholson et al. consider how age and lack of digital knowledge can act as a barrier to access [52], with work on the topic of assisted access for the elderly highlighting how security and privacy technologies are threaded through all forms of access [47].

Work at the intersection of HCI and security considers how digital assistance is provided to people in different communities, circumstances and contexts [4, 43, 82]. In particular, work has focussed on the role of informal support networks within the home, and the role *helpers* or *assisters* play in providing technical support or influencing security behaviours [14, 55, 58]. Nthala and Flechais, for example, discuss the role social relationships play in the information security of the home and how such relationships serve as informal support networks of security practices [55]. In a recent study, Nicholson et al. [54] discuss how they recruited, trained and supported older adults to become "CyberGuardians" within their local communities, and, once trained, the community educators would then go back to their local communities to promote best security practice and guidance to fellow elderly adults at risk from "opportunistic online attacks". Chouhan et al. demonstrate how communities and collective action can provide oversight and forms of community governance that support security decision making as part of digital access [14].

2.3 Assisted Access Through the Voluntary and Third Sector

Whilst the majority of the literature concerned with assisted access focuses on assistance in domestic settings, it has long been established that assistance can also occur in civic settings such as community centres and libraries [20, 57, 68]. Libraries in particular often have a mandate for fostering digital inclusion [20] and an important aspect of this is to reduce or remove the barriers to information retrieval [71]. Libraries are often focused on building skills related to information archival and retrieval [20, 57], and they are also becoming a place for general technical support issues rather than issues related solely to using the digital library services [57]. Kin, work and friendship networks are where people first turn for digital help, with libraries as an extension or replacement to those closer ties [41, 57]. The two main security themes in this canon of library studies literature are the preserving of privacy in information searches [20] and the adjustment of information seeking practices to avoid information that might cause an individual distress or trigger trauma [71].

Since the early 2000s, voluntary and third sector organisations in the UK have been providing digital support services similar to those offered by public libraries. Being part of such community organisations is an important means for vulnerable people to build social, economic and political capital by developing digital skills [36]. COVID-19 has foregrounded the extent to which voluntary and third sector organisations have had to support individuals and families in accessing essential services, but have often needed to do so remotely due to restrictions and not being in a familiar

community setting. Many community service providers have needed to deliver a blend of in-person and digital services to reduce the effects of exclusion [61]. Often, the safety and security of access to essential services in civic settings comes from the safety of the setting itself [68]. Informal assisted digital access is a form of relational service where both parties support each other and where help and support is moulded to the needs of the individual. As with all relational services, informal assisted digital access is a collaborative form of service that is characterised by *"the intensity of interpersonal relations [that are] required to enable such solutions to operate"* [15]. Relational services are particularly needed in marginalised and underserved communities [16], and informal assisted digital access enables the wider relational service that is being provided. It could be argued that a relational service is not only about assisting access but also about aligning an individual's understandings and perceptions of access with the security controls designed into the service. Such alignment has long been regarded as important for secure access: *"the human interface must be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly...[and] to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized"* [69]. The focus on 'mental image' speaks not only to the process and flow of a technological control, but also to the goals it is trying to reach. Relational services are also necessary to help individuals and groups build resilience to overcoming barriers to access [79].

However, despite the focus on assisted access and the importance of building different types of capital and means of assistance, digital services are still not designed for shared access [78] and this poses many challenges in the delivery of assisted digital access. The study described below sets out to identify the characteristics of safer assisted digital access, and examine how the design of digitally-delivered essential services hinders assisted access and what might be done to improve the situation.

3 STUDY DESIGN

Our study was designed with a view to understanding how voluntary and third sector organisations assist in digital access, and gain insight into how they secure themselves and those they are assisting during this process.

Motivation and recruitment. The researchers had reviewed reports on digital access during the early stages of the COVID-19 pandemic, and had kept in touch with their existing network of community groups to identify key areas of concern. The theme of assisted access was consistent in these reports and discussions. The research team discussed the theme as a possible study with the network of community groups, and three of these stepped forward to take part in a study. A further three community groups volunteered to take part, and these were not known to the research team prior to the study. The community groups are all voluntary and third sector organisations located in northern England. The participants were all community workers who provide community assistance as part of their day-to-day work. Combined, the groups assist in excess of 6,000 individuals per year. Table 1 below shows the groups typically assisted by our participant organisations.

Whilst the research team typically works on the ground with marginalised and underserved communities, the risk of COVID infection was decided to be too high at the time of the study. The joint decision was made by the researchers and participant groups to conduct the study on-line. Informal pre-study discussions were held with representatives from two of the five community groups, to ensure that the participants would find the study welcoming and supportive. This co-design of the study ensured that the study was framed in a way that was meaningful to the community groups, and created a space in which the community groups could articulate the issues that were important to them. The informal discussions emphasised that the topic of assistance is

1	Those needing support accessing housing, welfare and financial services.
2	Those accessing healthcare services.
3	Long-term unemployed, and those first experiencing welfare system.
4	Young people, receiving or leaving social care.
5	Autistic people, without learning disabilities.
6	Over-60s, pensioners.

Table 1. The six categories of participant in our study.

inherently complex, and understanding assistance required an understanding of economic and social precarity and that these precarities could be generalised for communities or groups of people.

Study Limitations: The study's recruitment of members of voluntary and third sector organisations limits the study in so far as the only assistance practices that were presented were the ones that the participating organisations see. The study is also limited in the sense that the experiences that are reported are from the perspective of the assisters rather than the assisted. However, working with the assisters offered the best route for obtaining quality data during the COVID-19 lockdown period. A sibling study with the assisted, taking place in-person, is planned as a complement to this study.

Study structure. Ahead of the session, the following primer was sent out to participants.

"During the workshop we want to hear your experiences of assisted digital access. Those experiences might be as someone who:

- *Receives assistance from friends and family to access digital services*
- *Provides assistance to friends and family members to access digital services*
- *Provides digital access assistance to people as part of your job*
- *Has to respond to problems and challenges resulting from assisted digital access"*

The purpose of the primer was to encourage reflection ahead of the session. In total, two sessions were conducted, each lasting two hours, conducted online via the video communication platform Zoom. Five community groups were engaged with, and a total of 9 people working for these groups attended the two sessions.

The study was conducted under the academic institution's ethics process and policy. The study was structured as shown in Table 2. In addition, several verbal prompts were designed, to be used at different stages of the sessions, and these are shown in Table 3.

Opening and closing discussions were facilitated by the lead researcher. Each small group consisted of 1-3 participants, facilitator and scribe. The latter made notes on the discussion and posted them to the chosen online storyboard format (as set out below). We used the term *"story"*, encouraging participants to share rich descriptions of assisted access as they have encountered it. Stories and storytelling are often a central component in participatory engagement and design [33] because they are a means for participants to bring their lived experience and cultural history to an engagement. In the case of assisted access, using the "story" form encouraged participants to articulate the social, cultural, economic, emotional and political entanglements that are woven through the process of accessing and using a digital service on behalf of another.

Choosing the Format. Moving to an online medium for the sessions was not an easy decision. Whilst online discussions had become a more regular occurrence for voluntary and third sector

STAGE	Breakdown
Pre-study alignment	Initial discussion with gatekeepers for our groups, concerning topics and forms of informal assisted access that might best be discussed with the groups.
Focus Group	2-hour session held on Zoom (including short break) exploring topics, examples and stories, to discover how these organisations approach assisted access. The session was divided into 3 segments: i) **Introductory discussion** (20 mins) on the nature of assisted access, for the benefit of the assembled groups as a whole. ii) **'Break-out' groups** (60 mins) looking at examples of assisted access. iii) **Plenary discussion** (40 mins) with the group as a whole to arrive at conclusions, sharing first impressions, experiences and insights that may have been gained from the session.
Feedback and Reporting	Notes were taken and insights and stories were written up; participants invited by email to review and provide feedback before being finalised and reported and shared again.

Table 2. The study structure.

workers, it was still not a default medium of communication for our participants. In order to get as close to face-to-face discussion as possible, the research team proposed an online format that encouraged collaborative discussion and where their contributions could be easily captured in a way that was open and easy to access and edit. It was also important that the medium was of no cost to access (e.g. did not require a licence), and that it possessed simple functionalities easy to navigate and use. In this way the participants could access the format without cost and "drive" the medium with little assistance. The researchers also wanted to select a medium that the community groups might find useful for future engagements of their own. After a review of possible platforms, Padlet, a cloud-based virtual bulletin board, was selected.

Data Capture and Analysis. Data was captured in two forms during the sessions: handwritten notes, and digital collage using Padlet. Padlet collaging was undertaken in the 'break-out' sub-group part of the main session. Each sub-group had a facilitator moderating the conversation, and a scribe capturing key discussion points mentioned by participants. Researchers and participants collaborated to add small images and arrows to help animate and bring further dimensions the stories and experiences described on the Padlet boards.

After the sessions, researchers added any additional notes to the collages that were necessary for context and legibility. The research team then sent a summary of the discussion points to each community group. This summary included a web-link to the final Padlet collage and an invitation for feedback. The research team followed up with the participant groups after 7 days.

STAGE	Prompt
Introductory discussion	**Opening prompt:** *"What are the ways in which you have assisted people in need of digital access?"*
'Break-out' sub-group	**Opening prompt:** *"Can you describe one of the most common assisted digital access stories that you come across day-to-day?"* **Unpacking the story**: *"In this story of assisted access, what makes the characters feel safe and secure?"* **Concluding prompt:** *"Can you tell us if there is any one thing that you would change, if you could, to make digital access more inclusive?"*
Plenary discussion	**Concluding prompt:** *"Is assisted digital access always going to be necessary, or can we design it out in any way?"*

Table 3. Verbal prompts used during the discussions at different stages.

The data captured via the Padlet boards and the notes taken by facilitators were subsequently independently analysed by two researchers on the team. The data was first analysed by grouping together emergent themes, using as a guide the different categories of verbally delivered prompts that stimulated the general and sub-group discussions (Table 3). Each Padlet board was sent back to the participants for review. The feedback was used to revise the Padlet boards and then the participant groups gave feedback on the revised Padlet boards. This process continued until all participants were satisfied. In the findings, large parts of the Padlet boards are reproduced.

In the sections below we set out our findings in two parts. Firstly, we set out the different types of assisted digital access that were reported during the sessions. This shows the complexity of assisted digital access. Secondly, we present the findings in terms of the characteristics that defined the assisted digital access provided by voluntary and third sector organisations. These characteristics were present across the spectrum of assisted digital access. The spectrum and characteristics combine to provide us with the dimensions of digital assisted access as carried out by voluntary and third sector organisations represented in this study.

4 FINDINGS: SPECTRUM OF ASSISTED DIGITAL ACCESS

Analysis of the responses captured in Padlet identified types of assisted access that voluntary and third sector organisations might undertake. In the following subsections we set out the different types of assisted digital access that were reported during the sessions. These different types of assistance also reflect the breadth of assistance roles that the voluntary and third sector participants reported undertaking.

4.1 Replacing a Family Assister

As the literature review highlighted, much of assisted digital access takes place through kin, work and friendship networks. However, this raises the difficult question of what happens when an assister

is no longer present, particularly in the case of the death of assister (Figure. 1). The participants gave examples of how COVID-19 had disrupted those support networks, making assistance from voluntary and third sector organisations more important. In one digital assistance story, a person lived alone within the support services' local housing support network, and, with little technological ability and experience themselves, relied heavily upon regular support from a family member. In particular, they relied on access given at the assister's home: *"Little technological ability/experience. Regularly assisted by parent/assister... Assister passes away. Relied on devices/internet at assister's house to access everyday services. Now this has gone = so has no access."* Without access to everyday services such as benefits, banking and medication, the vulnerable individual is in effect left by themselves and was *"left overwhelmed"* during a period of immense stress. The voluntary organisation steps in and begins to support the individual in gaining digital access.

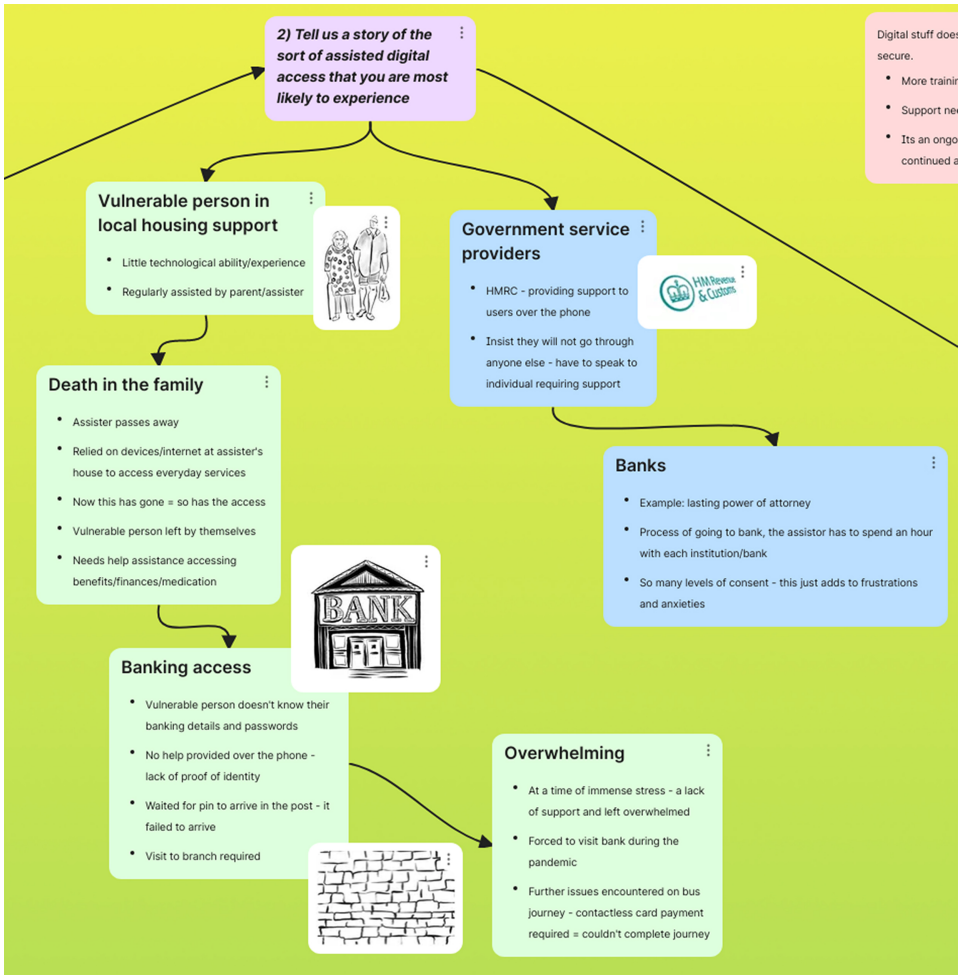

Fig. 1. Group One: A detail from one of the Padlet boards, describing how the death of a family member, who had routinely helped with access, left the assisted person with a difficult situation to deal with, without appropriate assistance from government and banking services.

4.2 Protecting The Vulnerable

Voluntary and third sector organisations have an important role in protecting the vulnerable against digitally facilitated scams, and our participants felt that education and awareness is a key means of doing this. However, it was also felt that education and awareness needed to be provided in a way that was relatable to the individual and in a way that was non-judgmental and empathetic. As shown in Figure. 2, participants discussed how it was often difficult to explain the dangers because digital harms were often seen as less immediate by the groups that the community workers worked with: *"A digital punch in the face is less obvious,"* and, *"Need to show the effects to people - it's hard to get a visceral feeling with digital... may need a victim to talk about it to make it real."*

One account was given of where an elderly woman had sent money overseas to what she had thought was a potential husband, only to then find out that this was not the case, and that her money had been lost: *"She knew what she was doing in some way, she just wanted to send the money"*, led on by a combination of loneliness and *"being needed/wanted."* Providing education and support to vulnerable people in these situations requires that the emotional backdrop is understood, as well as the technical know-how necessary for preventing such scams. Without the understanding of the emotional environment, the vulnerabilities remain and the technical responses are less effective.

4.3 Interface Between The Individual and The System

The voluntary and third sector workers often facilitated access by performing mediation and facilitation roles to find paths through systems (Figure. 3). For example, an account was given where an individual wanted to use their new name and gender when starting to enrol at a local college: *"A fresh start at college."* However, they wanted to remain in 'stealth' mode. This type of situation is complicated by the fact that an individual *"might be out as gay but not as trans, and out about different things to different people"*, hence the need for them to be able to manage their identity in appropriate ways. The individual found that the college administrative system stated that they were obliged to reveal their original gender. Unable to ask the college about how to best to fill out the paperwork (as this would 'out' the individual), the assister intervened and phoned the college; this revealed the existence of an ID number (that includes legal name, sex, gender) that follows a pupil from primary to college-level education: *"it's going to exist but he doesn't really want it to - an identity he doesn't identify with."* This is an example of a voluntary sector worker acting as an interface between an individual and the college regulatory environment. The legal and college regulatory environment is thus *"both a source of assurance and at times the problem."*

4.4 Proxy-Access at Scale

Providing proxy-access to essential services is a core digital assistance activity for all of the participants. For example, participants included a local community action group in the North East of England that provides monetary, debt and welfare advice and support to vulnerable groups (Figure. 4). As part of this support, the organisations completes online forms on behalf of individuals and households on a daily basis. Many of the experiences and stories shared were against the backdrop of the pandemic, where the service had experienced an extra 3000 new people and households newly added to their register looking for support. In order to respond to this uplift in numbers, processes and procedures were put in place to be able to act on behalf of another at scale.

4.5 Providing Infrastructure For Digital Access

Three of the participant groups provided the technological infrastructure (computers, data and connectivity) necessary to access digital services, as well as provide support to use the infrastructure. For example, one of the participant groups was a local housing charity (Figure. 5). On top of providing

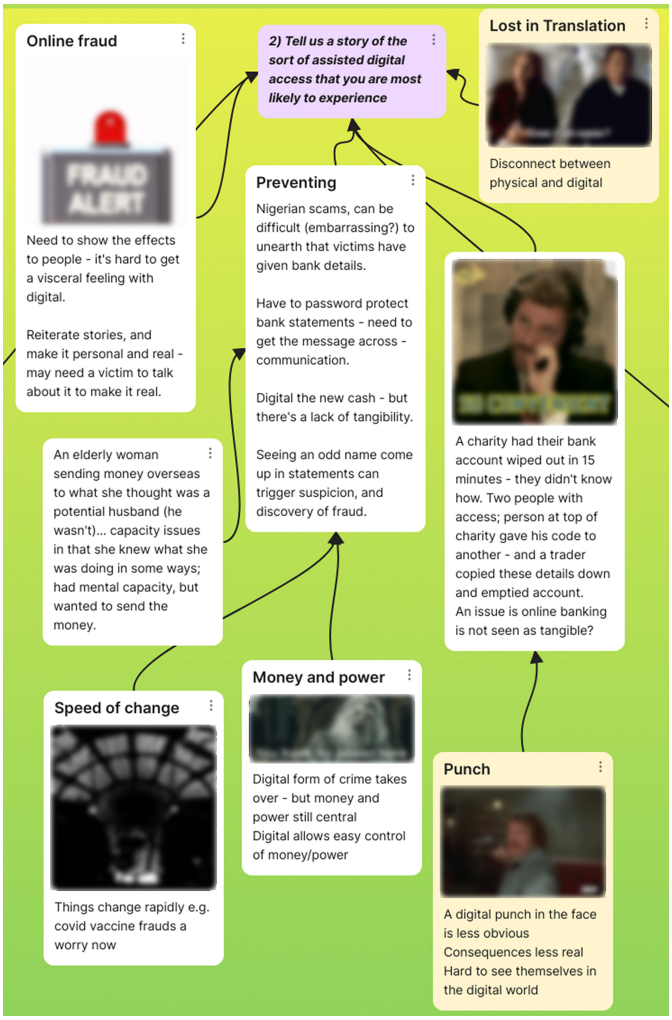

Fig. 2. Group Two: A detail from one of the Padlet boards, relating to issues of online fraud and vulnerable and isolated individuals, including older people.

housing support, the charity runs a computer project, where local tenants are assisted with various forms of technological support – from the provision of devices and smartphones, to the use of local online services such as job searches and booking healthcare appointments. To help tackle the precarity faced across their community regarding internet provision and access, the charity receives and donates refurbished tablets and smartphones to homes where there is an acute need. However, with the local telecommunications provider holding a monopoly over internet provision, tenants still face issues regarding affordable and unfettered internet access, resulting in limited data connectivity: *"We have huge ongoing issues with data. Our smartphones are pre-installed with 24GB of data - but what happens when this runs out?"*.

For many families helped by the charity, the lack of data and lack of access to devices made the required homeschooling during the pandemic virtually *"impossible on small/single devices"*, and this was exacerbated in multi-child households and where parents were required to work from home.

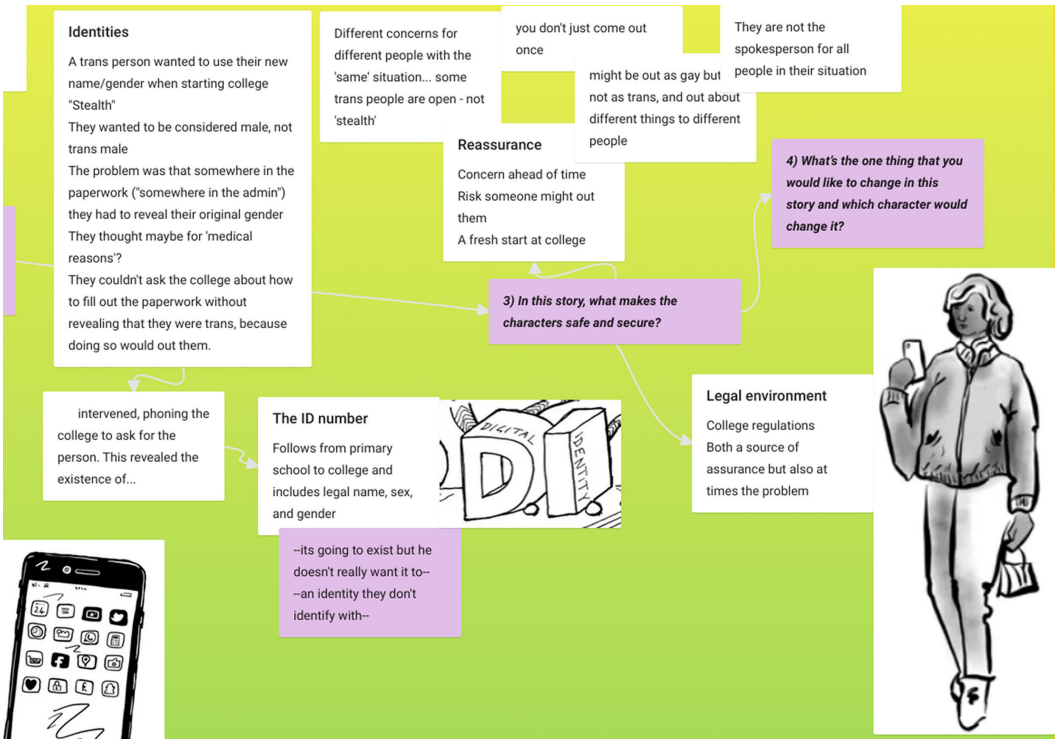

Fig. 3. Group Three: A detail from one of the Padlet boards, describing the issues encountered in managing identity and access for a trans person and their interactions with the education system.

In order to tackle ongoing issues around digital exclusion within their community, one participant (Figure. 4) called for *"digital equipment and accessibility"* to be *"made more widely available to those who are most vulnerable and who need it most."*

5 FINDINGS: KEY CHARACTERISTICS OF VOLUNTARY AND THIRD SECTOR ASSISTED DIGITAL ACCESS

In this section we set out the main characteristics that define the assisted digital access provided by voluntary and third sector organisations.

5.1 Operating From a Secure Foundation

Our findings showed that voluntary and third sector organisations were aware of the need to operate from a secure environment. Organisations recognised that they had to have policies and technological configurations that enabled them to operate safely and support vulnerable people as they accessed their support and help. For example, in the second group (Figure. 2), participants discussed a number of stories relating to issues of online fraud, from experiences of online dating scams to a social engineering attack against a charity organisation: *"A charity had their bank account emptied in 15 minutes... [a] person at top of organisation gave his code to another."*

Across our study, we found that many of the voluntary and third sector organisations have developed processes for supporting people at scale. These processes include gaining consent,

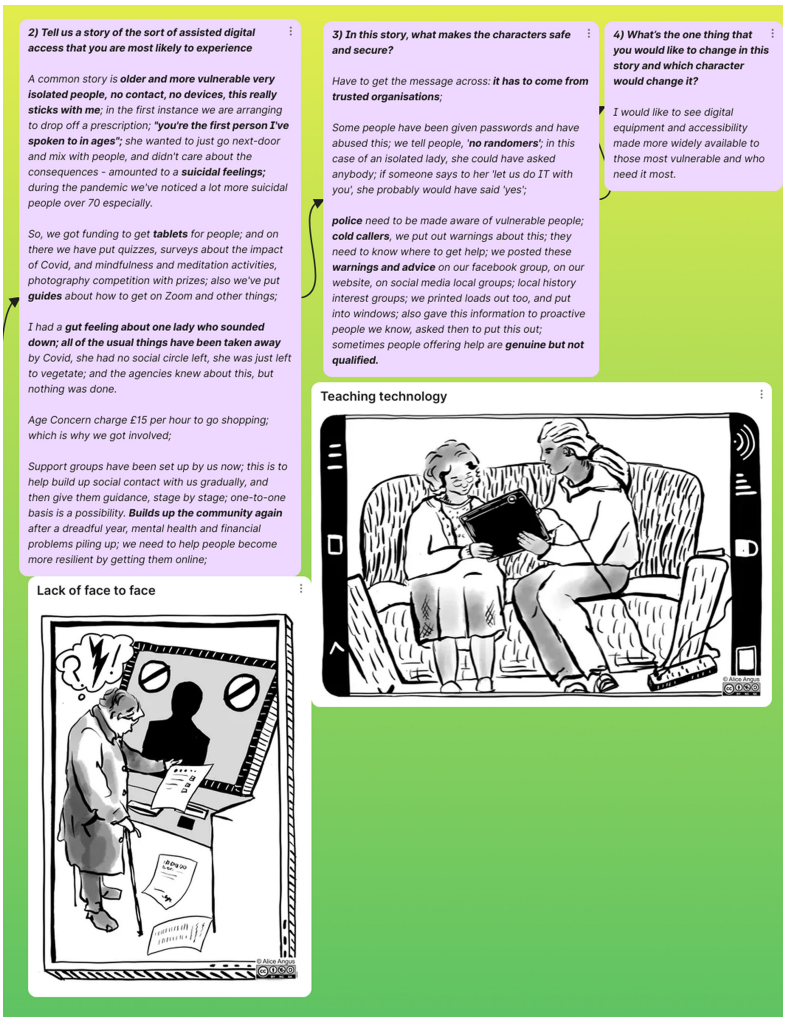

Fig. 4. Group Four: A detail from one of the Padlet boards, describing the activities of a local community action group in the North East of England that provides monetary, debt and welfare advice and support to vulnerable groups.

communicating effectively with other key organisations and public institutions, the secure storage of details and a processes for gathering necessary personal data (Figure. 4).

Regulations also provide a secure foundation. In the majority of cases, the voluntary and third sector organisations that participated in the study regarded such assistance as part of a wider safeguarding role that relates to their duties under the UK's Care Act (2014). In the case of one of the community organisations, they had a formal relationship with the Department of Work and Pensions (DWP) that authorised them to help people claim welfare via digital means. However, this arrangement was the exception.

Secure foundations also come from the values and principles of the assisters themselves. Assisted access is the outcome of a determination not to allow people to be "left by the wayside": *"Trust between tenant and us is key at almost every step. This gives them the peace of mind and confidence in*

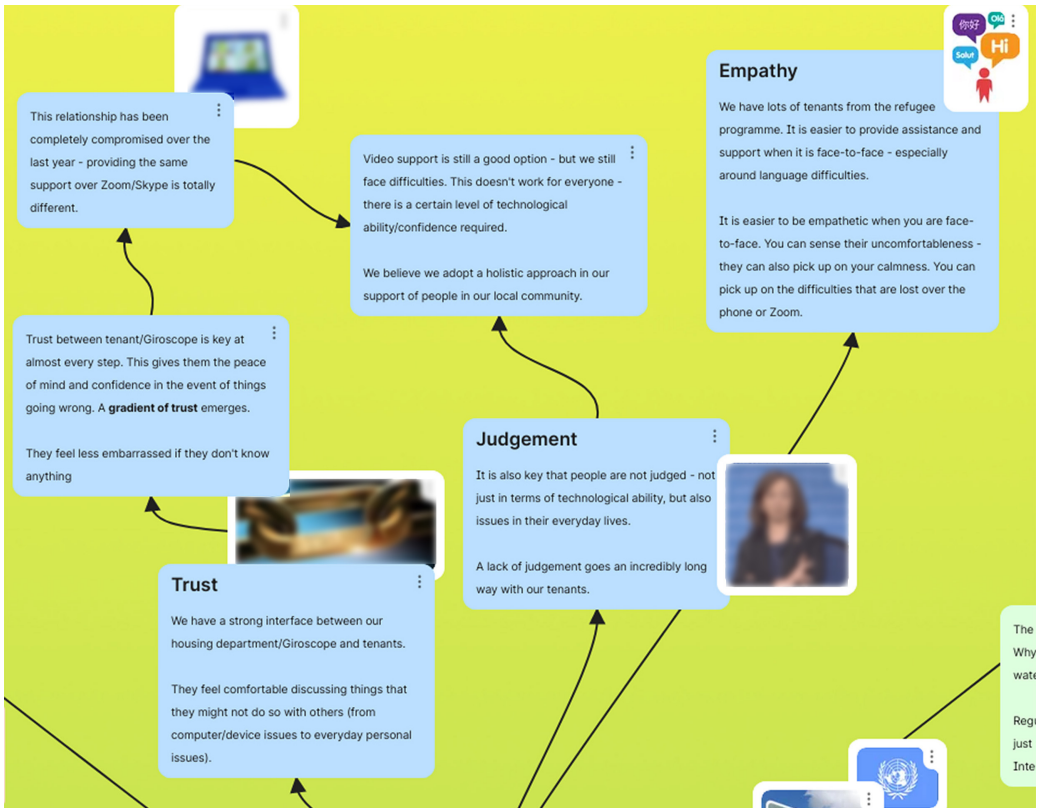

Fig. 5. Group Five: A detail from one of the Padlet boards, describing how a local housing charity receives and donates refurbished tablets and smartphones to homes where they are most needed, and assists access there.

the event of things going wrong. A gradient of emerging trust. They feel less embarrassed if they don't know anything." (Figure. 5).

5.2 Breadth and Complexity of Assistance

The stories that were divulged during the study reflect that assisted access has no clear boundaries and that digital assistance is a complex service woven into many day-to-day experiences. This is perhaps not surprising given that the need for assistance largely originates from a lack of skills, confidence and resources that result from economic and social deprivation (Figure. 5). Each story revealed that assistance is needed in all areas of life. Participants did not think in terms of assisting digital access but conceptualised access assistance as being enmeshed in a wider set of assistance and support activities. For example, one organisation was able to respond: *"So, we got funding to get tablets for people; and on there we have put quizzes, surveys about the impact of Covid, and mindfulness and meditation activities, photography competition with prizes; also we've put guides about how to get on Zoom and other things."*

Digital access often increases the range of risky activities that a vulnerable person carries out. These vulnerabilities often intersect with each other - for example, poverty typically intersects with lack of access to data and computers, which in turn might intersect with lack of digital skills. Rapid speed of change can also increase a person's vulnerability. As one of the Padlet boards shows

(Figure. 2), COVID-19 vaccine scams have become a means for fraudsters to extort money via digital means. COVID-19 has also become a significant vector of vulnerability, as the increased dependency on digital services can result in people having to trust a wider set of people for support and exert a real pressure to make those trust-related decisions at speed. Concerns were voiced that digital access was often requiring individuals to share personal information that could be intercepted and misused by a malicious third party, or by a purported trusted assister, such as a neighbour or member of the local community.

5.3 Assisters as Problem Solvers

Assisters spoke of the many types of barriers to providing assisted access, and of the need to solve particular problems in order to be able to deliver assistance. Such problems stemmed from lack of resources, the complexity of the services that needed to be accessed, and the sense that very often the voluntary and third sector organisations were not being recognised as legitimate sources of assistance. A considerable amount of problem-solving was related to voluntary and third sector organisations needing to gain recognition as legitimate assisters before being able to provide assistance to the individual. Whether dealing with the banks or dealing with the tax authorities, assisters had to spend a considerable amount of time negotiating access before they could assist the individual (Figure. 1). These problems were further compounded by the lack of direct access to the individual in person. As such, organisations described how, pre-COVID, providing assistance was easier because it could very often be provided face-to-face (Figure. 5). Providing assistance remotely requires an additional set of problems to be solved. Not being recognised as a legitimate assister can mean that assisters also have to overcome the problem of having limited or partial information (Figure. 3). Often, the assister finds themselves in the position of not knowing precisely what resources an individual has access to, or what their history is with a particular service provider.

Instances of where resource-constrained access increased problems related to assistance were given during the sessions. In many cases within families, individual family members were competing for critical access to the internet. Assisters had to resolve some of these problems by finding additional technology to donate to these families, ideally technology with enhanced functionality (Figure. 4 and 5). People are also vulnerable to rogue assisters and the increase in digital dependency will only increase this vulnerability (Figure 5). Some of these issues of reduced access were solved by assisters offering their own devices for access to services for specific tasks (Figure. 3), which in itself increase the vulnerabilities of both the assister and the assisted.

5.4 Networks of Assistance

As part of scaling up assistance, voluntary and third sector organisations build up networks of assistance (Figure. 4). This includes extending the web of assistance by gaining assistance from third parties, such as the police, by making them aware of who is particularly vulnerable (Figure. 4). This is one way of sharing the responsibility. The participants reported neighbourhood or community assistance networks emerging via social media as a result of COVID-19. Whilst such networks of assistance help to increase the capacity of support and rebuild a sense of community after COVID-19, the community group also reported their concern that such networks are harder to monitor and can place their individuals at risk of online manipulation and harm. Community groups gave examples of how people's vulnerabilities are being exploited by others - for example, fraudsters might fake offers of help to individuals to assist them with access to welfare claims or claiming a COVID-19 bursary. Examples were also given where individuals were being encouraged to make fraudulent welfare claims, where the manipulator takes a cut of the resulting money. In other cases, fraudsters might take money for providing assistance (as a paid service) in making

apparently legitimate welfare claims, but where funds are diverted to the fraudster or no claim is made.

5.5 Emotional Aspects of Assistance

The stories revealed that insecurity for the communities the organisations serve is not just about not having access to technology or the relevant digital skills - rather, insecurity also comes from social and physical isolation and a lack of social capital. As one participant explained: *"A common story is older and more vulnerable very isolated people, no contact, no devices, this really sticks with me; in the first instance we are arranging to drop off a prescription; [they say] 'You're the first person I've spoken to in ages'; she wanted to just go next-door and mix with people, and didn't care about the consequences - [this] amounted to suicidal feelings; during the pandemic we've noticed a lot more suicidal people, over 70 especially."* Solving the technical or skills component will not necessarily reduce the insecurity of the individual that needs to be assisted. The need for assistance is therefore not simply about the need to access a service, but also a need to build close supportive relationships with an individual. Assistance can be interpreted as taking an interest in someone, an interest which can make people feel valued. In contrast, being defrauded can have a long-lasting emotional (and economic) impact (Figure. 2).

Voluntary and third sector organisations also provide support when the situation feels too overwhelming for people to help themselves. The Padlet board shown in Figure. 1 documents particular difficulties around access to banking due to the individual not knowing passwords and being unable to provide proof of identity over the phone: *"No help provided over the phone - lack of proof of identity. Waited for PIN to arrive in the post - failed to arrive... Forced to visit bank during the pandemic. Further issue encountered on bus journey - contactless payment required = couldn't complete journey."* The lack of appropriate support from governmental and banking services can cause "immense stress" to an individual, and is often compounded by *"So many levels of consent - just adds to frustrations and anxieties."* Our participants noted that when people encounter problems, they often 'freeze' as they do not have the confidence to respond adequately and can easily become overwhelmed (Figure. 5). As our Padlet boards show, this sense of being overwhelmed can come from background stresses, as this comes together with the complexity of what is being asked, and the sense of heightened risk during the pandemic. These stories also show how digital assistance is needed in many circumstances, even during physical, face-to-face situations.

6 DISCUSSION

As we outlined in our literature review, security can be conceptualised in two modes: positive security (ability to live free from fear of security threats) and negative security (protection from security threats) [67]. Our findings show that voluntary and third sector organisations have developed security strategies for assisted digital access that combine 'positive' and 'negative' forms of security. On the one hand, organisations promote and implement digital security (negative security or protection from digital harms), while on the other they help individuals to build up social, political and economic capital so that they can realise the benefits of digital access (positive security, or 'freedom to' live free from fear of security threats). Organisations therefore help individuals to acquire e-safety and digital protection practices to securely build social, political and economic capital. At the same time, this capital enables individuals to enhance their digital protections. Voluntary and third sector organisations deploy this positive-first security strategy as a response to the conundrum: how to bring digital security to people who have inherently precarious lives? The people-centered security design literature, that encompasses usable security and inclusive and accessible forms of security technology, focuses on making security technologies more readily usable by a wider cross-section of the population. However, the connection between the security

of people and the digital security interaction itself is not typically addressed in the people-centred design literature. This study has brought to light some of the ways in which voluntary and third sector organisations are making this connection.

Our findings show that this positive-first security strategy has the following components:

- Providing access to internet and computer technology (physical and economic capital) to reduce insecurity from lack of such infrastructure.
- Knowledge transfer to develop 'know-how' capabilities, in skills and usage when accessing technologies.
- Building trust relations with communities, sustained high quality of assistance, underpinned by responsibility and social and political integrity (social and political capital).
- Providing assisters who are on the same side and fighting for the same goals (social capital).
- Providing assisters who show empathy, reliability and care (social capital).

In the paragraphs below we expand how these components and in each case, we tie the element of the strategy to both a role and characteristic of the assister, as set out in the findings.

Provision of Internet Access and Computer Technology: At the core of the security strategy is the provision of digital access. Our findings in the subsections *Breadth and Complexity of Assistance* and *Providing Infrastructure for Digital Access* show how the breadth of assistance that voluntary and third sector organisations provide is largely dependent on access to digital services. Three out of the five organisations we worked with regard providing access to digital infrastructure as a fundamental part of their work and that safer digital access starts with this provision. Typical security guidance practice guidance [50] assumes that people have access to digital technology and network connections. The literature surveyed for this paper also focused on support once technology and access to the internet are available. Yet our findings show that gaining and maintaining access to digital infrastructure is an on-going source of anxiety for assister and assisted alike: *"We have huge on-going issues with data. Our smartphones are pre-installed with 24GB of data - what happens when that runs out?"* (Figure. 5). The findings also show that the assisters understand the limitations of the assisted's resources and recognise how this changes the nature of the digital threats that the assisted face. The participants also recognised that access is shared, often through economic necessity. Such sharing requires requires a set of careful trusting practices. The assisters recognise that the precarity that the assisted experienced makes them particularly vulnerable to trusting people who show an interest in them: *"Perpetrators fill a need for a victim - something draws them in. Being needed/wanted can lead to vulnerability being exploited."* (Figure. 2).

Skills and Knowledge Transfer: Once the access to digital services has been achieved, the next stage in the security strategy is to transfer digital skills and knowledge to those that are being assisted. This includes security knowledge and skills. The findings in the subsections *Protecting the Vulnerable* and *Assisters as Problem Solvers* show, once physical access to a service is ensured, the assisters need to ensure that accessing online services does not increase the vulnerability of the assisted. Assisters in voluntary and third sector organisations are often characterised as problem solvers trying to reduce or re-frame problems to reduce the harms experienced by the vulnerable people they assist. One way this is achieved is to carry out online tasks on the assisted's behalf. Another way to achieve this is through knowledge and skills transfer. Aligned with the provision of technology and internet access is the transfer of skills. Such transfer builds confidence and self-efficacy which is fundamental to secure interactions. Our findings support existing work in this area [53, 53, 54], but shows that knowledge transfer needs to be framed in a way that the assisted find relatable. The findings show that skills are transferred by the assisters both showing

and telling the assisted how to securely access digital services and how to use the services in a way that derives benefit.

Our participants felt that government and business have a responsibility to ensure people are better informed and supported, especially when they are targeted by fraudulent activities, but that voluntary and third sector organisations need to do this if other institutions do not: *"Have to password-protect [your] bank statements - need to get the message across."* The findings reveal how both the assisters and the assisted are often dependent on the messaging from technology providers in order to reassure them of what needs to be done to securely complete transactions. One participant emphasised the importance of seeing things: *"Banking is now pushed on line but people like to 'see' things e.g. how much money they have, where transactions were made."* This need for seeing things equally applies to online protections, where people need to see what steps need to be taken and have it explained to them how it will affect them and their devices.

The voluntary and third sector organisations recognise that before people are able receive and process e-safety and other forms of digital knowledge and skills, confidence needs to be built up through social inclusion. For example, one of the groups explained: *"Support groups have been set up by us now; this is to help build up social contact with us gradually, and then guidance, stage by stage; one to one basis is a possibility."* (Figure. 4). As this example reveals, by reducing the economic pressure of accessing technology and connectivity, the assisters also reduce some of the anxiety related to digital access. This reduction provides a trusted and calmer space in which the assisted can both think through the protection steps they need to take to secure their access, and also creates a calmer space in which the assisted is able to take on board the advice of the assisters. Whilst the technical advice is important, the assisters also recognise that addressing some of the underlying vulnerabilities is important before the technical advice can be effective.

Trust, Responsibility and Integrity: Provision of access to digital infrastructure and transferring skills and knowledge are standard components of a security strategy. However, it is less common to find a security strategy that also has a component related to human values. As part of their security strategy, the voluntary and third sector organisations emphasised the importance of the values of trust, responsibility and integrity when supporting vulnerable people to securely access digital services. These values are reported in the findings subsection *Emotional Aspects of Assistance* and in the subsection *Breadth and Complexity of Assistance*. The findings reveal that third sector and voluntary organisations place as much emphasis on building secure relationships with the assisted as they do on ensuring access to digital infrastructure and skills transfer. This relationship building uses the human values of trust, responsibility and integrity to build a common understanding about why e-safety is necessary and how it helps to make the assisted less vulnerable.

Our findings show that whilst the quality of the relationship and the information that flows across that relationship is improved with trust, it is not trust alone that secures the assister-assisted relationship. Economic necessity and psychological well-being typically drive the assisted making initial contact and initially sharing personal data with the assisting organisation. In one example, an assister explained how the assisted often provided them with personal data and security details in order for the community group to gain access on their behalf (Figure. 4), and the voluntary organisation regards it as their responsibility and an act of their social and political integrity to ensure that this data is protected. It is the assister's sense of responsibility and doing the best for others that often maintains and strengthens the relationship: *"Builds up the community after a dreadful year, mental health and financial problems piling up, and we need to help people become more resilient by getting people online."* (Figure. 4). As trust develops between the assister and the assisted, it becomes easier for the assister to identify where help is needed. For example, one participant talked about the assisted *"Feeling less embarrassed if they don't know anything"* (Figure. 5).

Being On The Same Side: In order to assist vulnerable people, the assisters have to build a relationship with the assisted at speed. Often, the vulnerable are in urgent need of help. A key part of the security strategy is to demonstrate that the assisting organisation is on the same side as the assister. This means showing the assisters have similar life experiences, experiencing similar challenges. This reduces any tendency to reject advice or skills, encourages the vulnerable to accept help and makes it easier for the assisters to establish a common security goal with the assisted. The findings in the subsections *Replacing a Family Assister* and *Networks of Assistance* reflect how the assisters are both part of the same communities as the assisted, but also have many of the same digital exclusion experiences in their own lives. The traditional digital security guidance focuses on technical knowledge transition where information is given from experts to those that have less expertise or who are regarded as non-experts. The information exchange works in a different way between assister and assisted where a shared set of experiences are often used to frame advice and where there is a joint security goal shared by the assister and the assisted. For example, in Figure. 2, one of the assisters gives an example of having a mother in hospital and seeing how she struggles to pay the bills online from her hospital bed. In particular, the assister saw how difficult it was for his mother to use two-factor authentication. Eventually, the assister and his mother set-up power of attorney but that was also complicated from the hospital bed. The examples in our work show that as they are part of the same community, the assisted can more easily tap into the social, economic and political capital that the assisers have.

Being part of the same community offers potential solutions too. One voluntary and third sector organisation called for a recognition of the close relationship between the assisted and the assister through a vouching scheme. In Figure. 1, the assisters suggest a vouching scheme whereby banks enable the assisted to nominate someone from within their own community to vouch for them as a means to help with identifying and verifying the assisted's identity. In this example, the assister is suggesting that the voluntary and third sector organisations that support the assisted could act as vouchers.

Showing Empathy: Another important part of the security strategy is to show empathy for the assisted. This empathy helps the assisters to recognise the types of e-safety that are most necessary in each case and to recognise when intervention is needed. Our findings in the subsection *Emotional Aspects of Assistance* show that empathy, patience and reliability need to be demonstrated in the provision of secure assistance. One assister explained: *"I had a gut feeling about one lady who sounded down. All the usual things had been taken away by Covid. She had no social circle left, she was just left to vegetate; the agencies knew about this but nothing was done."* (Figure 4). The common theme of empathy is consistent across our findings. The findings show that assisters hold a number of common personal characteristics: from empathy, understanding and a degree of patience, to sense of reliability and assurance for the assisted. The assisters show an understanding of why on-line safety guidance does not always work and have suggestions for ways in which guidance and e-safety measures could be more effective. For example, one assister explains: *"When using contactless spending, sometimes vulnerable people can't remember how much they have spent. So when a payment has been made, send a text message to the individual telling them they have spent 'x' amount."* (Figure 1).

Empathy, patience and reliability are characteristics grounded in the professional personas that voluntary and third sector workers identify with. What is striking is that these characteristics were deployed for all types of assistance, regardless of who needs to be assisted. Previous research identified that certain groups are more likely to be assisted with empathy than others [47], but our findings show that voluntary and third sector organisations show empathy to a wide cross-section of the vulnerable in society.

Security of the Assister: The assisters recognise that for their security strategy to succeed, they need to consider their own digital security practices. Our findings do reveal some of the security practices that the assister undertakes. In the subsections *Operating from a Secure Foundation* and *Proxy Access at Scale* the security approach of the assister is discussed. In its programme of cyber security advice, NCSC also has security advice and guidance for small organisations [51] and charities [49]. However, it is noticeable that the assisters do not refer to the technical security of their own environments but do refer to the policies that they deploy to ensure that personal data is handled correctly. The importance of strong policy and process was highlighted with this comment: *"One charity had their bank account wiped out in 15 minutes - they didn't know how. Two people with access; a person at the top gave his code to another."* Whilst much of our findings focus on the protection of the assisted, this example shows that protection of the assister is also an important aspect of safer assisted digital access.

6.1 Design Principles for Safer Assisted Digital Access

From our findings we can identify a number of design principles that could be included in digital service design to facilitate safer assisted digital access. These design principles promote a positive-first security approach for both assisters and the assisted. The principles include accessible and inclusive technology and reflect the importance of people-centered design. However, the design principles also reflect that people-centered design and accessible and inclusive digital technology is insufficient on its own to support safer assisted digital access.

Vouching: A clear message from across all the participant groups is the need for a vouching capability where the vouching can take place from within the community. There needs to be a function within essential, day-to-day services that allows for an individual to nominate a voucher to help with setting up and managing services. The voucher might undergo additional security checks and can be verified by the service provider, but the individual must have some agency to choose their own voucher. These vouchers are not simply administrative proxies but also have a duty of care, and a responsibility to watch over and provide care-ful assistance to the assisted.

Accessible interfaces and processes: All participant groups gave examples of how both the technology and the underlying administrative processes were often difficult to follow. There is much in the HCI and CSCW literature about accessible technologies, but principles of accessibility and inclusion need to also address and be implemented in the underlying processes for everyday essential services. This also means that the security principles need to be designed into the underlying services and that such principles must also be inclusive and accessible.

Support for dual use: In many cases, the assisters are working alongside the assisted as a form of proxy access. Supporting proxy access is not only a technology design question but, as the findings show, also requires changes to the underpinning process and policy model. There are currently no standard ways to recognise this type community assistance and, as a result, this leaves the assisters unrecognised, without a legitimate role, and leaves the assisted with a binary choice of accepting the assistance or not - without any clear means of auditing what assistance has been given.

Informative messages: The examples given by the participants show the importance of informative and relatable messaging as part of the digital service offering. The examples given by our participants showed that messages are important for informing people what they need to do to safely access services. The examples also showed that these messages need to be available at the point of need. To establish where the points of need are for vulnerable groups requires careful co-design that establishes how such groups and their assisters interact with digital services, and at which points security messaging is needed.

Networks of support: The traditional e-safety guidance largely assumes independent access where individuals have a one-to-one relationship with their devices. The findings show how for vulnerable, underserved communities access is often a networked activity where digital resources are shared and support comes from a wide variety of sources. E-safety and cyber security guidance for individuals should reflect the roles of networks of support and the security practices related to this support.

7 CONCLUSION

The more societies become dependent on digital communications, the more important it is that secure digital access is available to all parts of society. Our study shows how voluntary and third sector organisations place traditional digital security and e-safety guidance in a multi-dimensional view of the full security terrain. Nuanced pictures of security, such as those described in our findings, are currently missing from the usable and people-centred security literature. This indicates that whilst user-centered design of security controls is necessary for safe digital access, it cannot be sufficient. We argue instead that an effective assisted access approach needs to includes elements of negative security but the overall approach needs to be led from a positive security position.

8 ACKNOWLEDGMENTS

We would like to thank the community groups who took part. We also thank Alice Angus for the line drawings included in the padlet collages. Heath's contribution received funding from the AHRC-UKRI Audiences of the Future Programme AH/S003622/1. Coles-Kemp's and Robinson's contributions were funded by the "Everyday safety-security for everyday services" fellowship programme funded by EPSRC EP/N02561X/1. We thank the RISCS Digital Responsibility Fellowship for hosting the workshop reported in this paper. The data underpinning this paper can be accessed at: DOI 10.17637/rh.20259045 For the purpose of open access, the author(s) has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.
[2] Andrew A Adams and Shirley A Williams. 2014. What's yours is mine and what's mine's my own: joint accounts and digital identity. *ACM SIGCAS Computers and Society* 44, 1 (2014), 15–26.
[3] Age UK. 2021. Digital inclusion and older people — how have things changed in a Covid-19 world? Online Briefing Paper. https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/active-communities/digital-inclusion-in-the-pandemic-final-march-2021.pdf Accessed: 2021-05-02.
[4] Jennifer M Allen, Leo Gugerty, Eric R Muth, and Jenna L Scisco. 2013. Remote Technical Support Requires Diagnosing the End User (Customer) as well as the Computer. *Human–Computer Interaction* 28, 5 (2013), 442–477.
[5] Axelle Asmar, Leo Van Audenhove, and Ilse Mariën. 2020. Social Support for Digital Inclusion: Towards a Typology of Social Support Patterns. *Social Inclusion* 8, 2 (2020), 138–150.
[6] Belén Barros Pena, Bailey Kursar, Rachel E Clarke, Katie Alpin, Merlyn Holkar, and John Vines. 2021. " Pick Someone Who Can Kick Your Ass"-Moneywork in Financial Third Party Access. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–28.
[7] Belén Barros Barros Pena, Bailey Kursar, Rachel E Clarke, Katie Alpin, Merlyn Holkar, and John Vines. 2021. Financial Technologies in the Cycle of Poor Mental Health and Financial Hardship: Towards Financial Citizenship. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–16.
[8] Andrew A Bayor, Margot Brereton, Laurianne Sitbon, Bernd Ploderer, Filip Bircanin, Benoit Favre, and Stewart Koplick. 2021. Toward a Competency-based Approach to Co-designing Technologies with People with Intellectual Disability. *ACM Transactions on Accessible Computing (TACCESS)* 14, 2 (2021), 1–33.
[9] Joseph Bonneau and Sören Preibusch. 2010. The Password Thicket: Technical and Market Failures in Human Authentication on the Web.. In *WEIS*.
[10] Stacy M Branham and Shaun K Kane. 2015. Collaborative accessibility: How blind and sighted companions co-create accessible home spaces. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2373–2382.

[11] Pam Briggs and Lisa Thomas. 2015. An inclusive, value sensitive design perspective on future identity technologies. *ACM Transactions on Computer-Human Interaction (TOCHI)* 22, 5 (2015), 1–28.

[12] Daniel Calderon Gomez. 2020. The third digital divide and Bourdieu: Bidirectional conversion of economic, cultural, and social capital to (and from) digital capital among young people in Madrid. *New Media & Society* (2020), 1461444820933252.

[13] Priyank Chandra. 2021. Piracy and the Impaired Cyborg: Assistive Technologies, Accessibility, and Access. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–21.

[14] Chhaya Chouhan, Christy M LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J Wisniewski. 2019. Co-designing for community oversight: Helping people make privacy and security decisions together. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–31.

[15] Carla Cipolla. 2012. Solutions for relational services. *Service design with Theory* (2012), 37–44.

[16] Carla Cipolla and Ezio Manzini. 2009. Relational services. *Knowledge, Technology & Policy* 22, 1 (2009), 45–50.

[17] Lizzie Coles-Kemp and Claude P. R Heath. 2020. Digital Identity: Ground-up Perspectives.

[18] Cédric Courtois and Pieter Verdegem. 2016. With a little help from my friends: An analysis of the role of social support in digital inequalities. *New media & society* 18, 8 (2016), 1508–1527.

[19] Lorrie Faith Cranor and Simson Garfinkel. 2005. *Security and usability: designing secure systems that people can use.* " O'Reilly Media, Inc.".

[20] Amber L Cushing. 2016. "If it computes, patrons have brought it in": Personal information management and personal technology assistance in public libraries. *Library & Information Science Research* 38, 1 (2016), 81–88.

[21] Matthew Davidson, Karen Renaud, and Shujun Li. 2014. jCAPTCHA: accessible human validation. In *International Conference on Computers for Handicapped Persons*. Springer, 129–136.

[22] Tawanna R Dillahunt, Matthew Garvin, Marcy Held, and Julie Hui. 2021. Implications for Supporting Marginalized Job Seekers: Lessons from Employment Centers. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing*.

[23] Paul DiMaggio, Eszter Hargittai, Coral Celeste, Steven Shafer, et al. 2004. From unequal access to differentiated use: A literature review and agenda for research on digital inequality. *Social inequality* 1 (2004), 355–400.

[24] Roxanne Lynn Doty. 1998. Immigration and the Politics of Security. *Security studies* 8, 2-3 (1998), 71–93.

[25] Paul Dunphy, Andrew Monk, John Vines, Mark Blythe, and Patrick Olivier. 2014. Designing for spontaneous and secure delegation in digital payments. *Interacting with Computers* 26, 5 (2014), 417–432.

[26] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the experience-centeredness of privacy and security technologies. In *Proceedings of the 2014 New Security Paradigms Workshop*. 83–94.

[27] Serge Egelman, AJ Bernheim Brush, and Kori M Inkpen. 2008. Family accounts: A new paradigm for user accounts within the home environment. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*. 669–678.

[28] Valerie Fanelle, Sepideh Karimi, Aditi Shah, Bharath Subramanian, and Sauvik Das. 2020. Blind and Human: Exploring More Usable Audio {CAPTCHA} Designs. In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)*. 111–125.

[29] Gunhild Hoogensen Gjørv. 2012. Security by any other name: negative security, positive security, and a multi-actor security approach. *Review of international Studies* 38, 4 (2012), 835–859.

[30] Good Things Foundation. 2021. A new manifesto for digital inclusion. Web page. https://www.goodthingsfoundation.org/insights/new-manifesto-digital-inclusion/ Accessed: 2021-05-02.

[31] João Guerreiro, Dragan Ahmetovic, Daisuke Sato, Kris Kitani, and Chieko Asakawa. 2019. Airport accessibility and navigation assistance for people with visual impairments. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–14.

[32] Xinning Gui, Yu Chen, Yubo Kou, Katie Pine, and Yunan Chen. 2017. Investigating support seeking from peers for pregnancy in online health communities. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–19.

[33] Christina N Harrington. 2020. The forgotten margins: what is community-based participatory health design telling us? *Interactions* 27, 3 (2020), 24–29.

[34] House of Lords Select Committee on COVID 19, UK Parliament. 2021. Select Committee on COVID-19. Corrected oral evidence: Living online. https://committees.parliament.uk/oralevidence/1736/pdf/ Accessed: 2021-05-02.

[35] Joey Chiao-Yin Hsiao and Tawanna R Dillahunt. 2018. Technology to support immigrant access to social capital and adaptation to a new country. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–21.

[36] Julie Hui, Nefer Ra Barber, Wendy Casey, Suzanne Cleage, Danny C Dolley, Frances Worthy, Kentaro Toyama, and Tawanna R Dillahunt. 2020. Community collectives: Low-tech social support for digitally-engaged entrepreneurship. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–15.

[37] Justine Humphry. 2014. The importance of circumstance: digital access and affordability for people experiencing homelessness. *Journal of Telecommunications and the Digital Economy* 2, 3 (2014), 55–1.
[38] Philip G Inglesant and M Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the sigchi conference on human factors in computing systems*. 383–392.
[39] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. 2016. Caring about sharing: Couples' practices in single user device access. In *Proceedings of the 19th International Conference on Supporting Group Work*. 235–243.
[40] Helen Jiang. 2020. Security for People with Mental Illness in Telehealth Systems: A Proposal. *arXiv preprint arXiv:2008.03406* (2020).
[41] Jamie Johnston. 2016. Conversation-based programming and newcomer integration: A case study of the Språkhörnan program at Malmö City Library. *Library & information science research* 38, 1 (2016), 10–17.
[42] Vaishnav Kameswaran and Srihari Hulikal Muralidhar. 2019. Cash, Digital Payments and Accessibility: A Case Study from Metropolitan India. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.
[43] M Krämer, W Seymour, and I Flechais. 2020. Responsibility and privacy: Caring for a dependent in a digital age. (2020).
[44] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. " She'll just grab any device that's closer" A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 5921–5932.
[45] Michelle L Mazurek, JP Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, et al. 2010. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 645–654.
[46] Nora McDonald and Helena M Mentis. 2021. Building for 'We': Safety Settings for Couples with Memory Concerns. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–11.
[47] Tamir Mendel and Eran Toch. 2019. My mom was getting this popup: Understanding motivations and processes in helping older relatives with mobile security and privacy. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 4 (2019), 1–20.
[48] Maggie Morgan, Vicki Hanson, Chris Martin, Janet Hughes, and Alan Newell. 2008. Accessibility Challenge-a Game Show Investigating the Accessibility of Computer Systems for Disabled People. In *CHI'08 extended abstracts on Human factors in computing systems*. 2609–2610.
[49] NCSC. 2019. Small Charity Guide. https://www.ncsc.gov.uk/collection/charity Accessed:21-04-2022.
[50] NCSC. 2021. The NCSC's cyber security advice to protect you and your family, and the technology you rely on. https://www.ncsc.gov.uk/section/information-for/individuals-families Accessed:17-04-2022.
[51] NCSC. 2021. Small & medium sized organisations. https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations Accessed:17-04-2022.
[52] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. " 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*. 1–11.
[53] James Nicholson and Jill McGlasson. 2020. CyberGuardians: improving community cyber resilience through embedded peer-to-peer support. In *Companion Publication of the 2020 ACM designing interactive systems conference*. 117–121.
[54] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and Embedding Cybersecurity Guardians in Older Communities.. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15.
[55] Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 63–82.
[56] Ihudiya Finda Ogbonnaya-Ogburu, Kentaro Toyama, and Tawanna R Dillahunt. 2019. Towards an effective digital literacy intervention to assist returning citizens with job search. In *Proceedings of the 2019 CHI conference on Human factors in computing systems*. 1–12.
[57] Heidi Kristin Olsen, Roswitha Skare, and Andreas Vårheim. 2020. Digital hjelp på biblioteket. *Rød mix: Ragnar Audunson som forsker og nettverksbygger* (2020).
[58] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E Grinter, and W Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 739–748.
[59] Massimo Ragnedda and Maria Ruiu. 2017. Social capital and the three levels of digital divide. (2017).
[60] Massimo Ragnedda and Maria Laura Ruiu. 2020. *Digital capital: A Bourdieusian perspective on the digital divide*. Emerald Group Publishing.
[61] Anita Ramsetty and Cristin Adams. 2020. Impact of the digital divide in the age of COVID-19. *Journal of the American Medical Informatics Association* 27, 7 (2020), 1147–1148.
[62] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 931–936.

[63] Karen Renaud. 2021. Accessible Cyber Security: The Next Frontier?. In *ICISSP*. 9–18.
[64] Karen Renaud, Graham Johnson, and Jacques Ophoff. 2021. Accessible authentication: dyslexia and password strategies. *Information & Computer Security* (2021).
[65] Jahmeilah Roberson and Bonnie Nardi. 2010. Survival needs and social inclusion: Technology use among the homeless. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work*. 445–448.
[66] Laura Robinson, Jeremy Schulz, Aneka Khilnani, Hiroshi Ono, Shelia R Cotten, Noah Mcclain, Lloyd Levine, Wenhong Chen, Gejun Huang, Antonio A Casilli, et al. 2020. Digital inequalities in time of pandemic: COVID-19 exposure risk profiles and new forms of vulnerability. *First Monday* 25, 10 (2020).
[67] Paul Roe. 2008. The 'value'of positive security. *Review of international studies* 34, 4 (2008), 777–794.
[68] Maria Laura Ruiu and Massimo Ragnedda. 2016. Between digital inclusion and social equality: the role of public libraries in Newcastle upon Tyne. *Library and Information Research* 40, 123 (2016), 69–87.
[69] Jerome H Saltzer and Michael D Schroeder. 1975. The protection of information in computer systems. *Proc. IEEE* 63, 9 (1975), 1278–1308.
[70] M Angela Sasse. 2013. "Technology Should Be Smarter Than This!": A Vision for Overcoming the Great Authentication Fatigue. In *Workshop on Secure Data Management*. Springer, 33–36.
[71] Reijo Savolainen. 2016. Approaches to socio-cultural barriers to information seeking. *Library & information science research* 38, 1 (2016), 52–59.
[72] Kjeld Schmidt and Liam Bannon. 1992. Taking CSCW seriously. *Computer Supported Cooperative Work (CSCW)* 1, 1 (1992), 7–40.
[73] Neil Selwyn. 2004. Reconsidering political and popular understandings of the digital divide. *New media & society* 6, 3 (2004), 341–362.
[74] Neil Selwyn, Stephen Gorard, and John Furlong. 2005. Whose Internet is it anyway? Exploring adults'(non) use of the Internet in everyday life. *European Journal of Communication* 20, 1 (2005), 5–26.
[75] Kristen Shinohara and Jacob O Wobbrock. 2016. Self-conscious or self-confident? A diary study conceptualizing the social accessibility of assistive technology. *ACM Transactions on Accessible Computing (TACCESS)* 8, 2 (2016), 1–31.
[76] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 895–904.
[77] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. 2019. Tough times at transitional homeless shelters: Considering the impact of financial insecurity on digital security and privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.
[78] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I Hong, and Laura Dabbish. 2019. Normal and Easy: Account Sharing Practices in the Workplace. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–25.
[79] Dhaval Vyas and Tawanna Dillahunt. 2017. Everyday resilience: Supporting resilient strategies among low socioeconomic status communities. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–21.
[80] Yang Wang. 2017. The third wave? Inclusive privacy and security. In *Proceedings of the 2017 New Security Paradigms Workshop*. 122–130.
[81] Yang Wang. 2018. Inclusive security and privacy. *IEEE Security & Privacy* 16, 4 (2018), 82–87.
[82] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. " We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.
[83] Earnest Wheeler and Tawanna R Dillahunt. 2018. Navigating the job search as a low-resourced job seeker. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–10.
[84] Mary Ellen Zurko and Richard T Simon. 1996. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*. 27–33.

Received January 2022; revised April 2022; accepted August 2022