Recognising diversity in older adults' cybersecurity needs

Benjamin Alan Morrison
James Nicholson
Lynne Coventry
Pam Briggs

http://dx.doi.org/10.1145/3582515.3609565

Recognising Diversity in Older Adults' Cybersecurity Needs

Dr Benjamin A Morrison*

PaCT Lab, Northumbria University, Benjamin.a.morrison@northumbria.ac.uk

Dr James Nicholson

PaCT Lab, Northumbria University, James.nicholson@northumbria.ac.uk

Professor Lynne Coventry

Abertay University, l521057@abertay.ac.uk

Professor Pam Briggs

PaCT Lab, Northumbria University, p.briggs@northumbria.ac.uk

Older adults continue to be targeted by cybersecurity attacks: a trend which shows no signs of slowing, and one that has become even more problematic given that many older adults adopted new digital technologies during the Covid-19 lockdowns. Yet there remains a scarcity of solutions designed to help older adults protect themselves online. In part, this is due to a lack of understanding of the specific needs of older adults, who are the fastest growing, and arguably most technologically diverse population on the internet. This study draws upon recent qualitative research to identify key dimensions which are likely to influence older adult cybersecurity behaviour and subsequent vulnerability. We show how these dimensions can be used, for example, to develop a wide range of personas that help illustrate the range of abilities and attitudes in the older adult population. The dimensions outlined here can be used to help researchers, designers, and developers better understand the diverse needs of older adult users when developing digital or security solutions for this population.

CCS CONCEPTS • Security and privacy ~ Human and societal aspects of security and privacy ~ Social aspects of security and privacy • Human-centred computing ~ Human computer interaction (HCI) ~ HCI design and evaluation methods ~ User models

Additional Keywords and Phrases: Ageing, Older adults, Cybersecurity, Personas, Diversity

1 INTRODUCTION

Older adults demonstrate the highest year-on-year adoption of internet-enabled technologies [15, 51] for many reasons ranging from leisure and admin, through to maintaining independence for longer in later life [8, 60]. The Covid-19 pandemic and its associated lockdowns rapidly accelerated technology adoption for many older adults [22] for reasons such as maintaining social interaction, accessing health services, and obtaining basic amenities such as food through online shopping [61].

Though beneficial for many, the rapid increase in technology adoption has also promoted increased risk, and researchers have begun to identify specific cyber-vulnerabilities for older adults [48, 62] who are increasingly targeted by cyber-attacks [1, 47], something which is evidenced by the rapid increase in online fraud during Covid-19 lockdowns [34]. It is, therefore, more important than ever to understand security vulnerabilities in the older adult population. However, one problem with achieving this goal is that older adults are too often considered as a single homogenous group, based on broad, age-related generalizations [20, 64]. To make progress in this area, we first need to recognize that older adults make up a highly diverse population.

Personas can help us achieve this goal. Personas are hypothetical representations of users which help stakeholders build empathy with users and consider wider audiences as a result of their attributes [44]. Personas have been used extensively within user-centred design since their introduction in the late 1990's [10], but were first adapted to cybersecurity settings by Stoll et al. [65] who used them to demonstrate how security visualizations could be used to help create more usable systems. Since then, personas have been used widely to better understand diversity across user groups such as students [5] and millennials [32]. Despite their usefulness, very little research has developed older adult personas, and even less has explored the diversity of the older adult population with regards to their technology use and nuanced issues, although a recent exception to this is Petrie's use of a range of pastiche personas as a light touch means of illustrating diversity [53].

In this paper we develop an evidence-based set of dimensions that can be used to generate personas that represent a varied set of older adult technology users. We draw upon recent, published, qualitative cybersecurity research to identify key characteristics likely to influence older adult security behaviours. We then use these as dimensions to develop personas which demonstrate some of the variability within this population, something which can be used to better understand the breadth and complexity of the security needs in this group. Our contributions are threefold: Firstly, we counteract age-based stereotypes of older adult technology users by highlighting the diversity of technological ability and technology use amongst this group of users. Secondly, we outline six key dimensions identified within recent older adult cybersecurity literature which can be used as to generate any number of personas likely to represent real-world older adult users. Thirdly: we provide designers, developers, and policy makers with examples of evidence-based personas generated using these dimensions. As a result, we hope to contribute to those who are seeking to be more inclusive when designing or developing solutions for older adult users.

2 BACKGROUND

Older adults remain the fastest-growing group of internet users worldwide, with over 75% of those over 65 now frequent users of the internet [15]. Many, but by no means all of these older adults are new adopters of technology, and as such, are still developing their digital literacy. Like most user groups, older adults utilize technology for a number of reasons [9, 25], but also have more esoteric uses such as maintaining independence in later life [13, 60]. Events such as recent global Covid-19 pandemics, and their related social isolation during 'lockdowns' have prompted even reluctant users to adopt technology to maintain social interaction, maintain contact with services and organizations [16], and access critical help [22].

While some older adults have the appropriate digital skillsets to benefit from technology use, many do not, and those most in need of support, i.e. those who do not fully understand how to stay safe online, are the least likely to receive it: a digital catch-22 [11]. These users are also the most likely to become victims of cyber-attacks. For example, recent research [48] has reported that older adults are at increased risk of online threats such as phishing, ransomware and online misinformation, and are disproportionally targeted by various internet scams and email attacks [1, 62].

2.1 Ageism and Stereotypes About Older Adult Users

Even though research has identified that older adults are more vulnerable to cyber-attacks, it is important to move away from ageist stereotypical conceptions of older adults as a single homogeneous group with poor digital literacy skills [67]. Ageist thinking has a number of consequences [38, 67], and stereotypes surrounding older adult technology use can hinder the effectiveness of technical and behavioural security solutions seeking to promote cybersecurity. The academic literature overwhelmingly focuses on chronological age when seeking to better understand older adults [46], which not only impacts the usefulness of the research, but also risks research ageism [71]. Few studies acknowledge that the older adult population is as diverse as any other age group, and indeed, when work, lifestyle and health factors are considered, this population could easily be considered the most diverse. Many older adults are keen to adopt and use technology [4], some feel forced into using technology [39] and others simply refuse to use technology [36]. One way to highlight, reflect upon, and counteract the negative stereotypes within our own field of HCI is to consider recent literature in this space.

Generalizations and ageist rhetoric is harmful. Mariano et al. [37] demonstrated that stereotype threat is negatively related to perceived ease of use, suggesting that older adults underuse technology because of a fear of validating negative stereotypes about them. Worryingly, it is likely that similar damaging consequences emerge when products and services are designed in non-inclusive ways, causing increased difficulty for some older adults, or excluding them altogether. It is unlikely that developers, designers, or researchers intentionally design *against* older adults, but it is important to recognize when our own unconscious biases and stereotypes lead to solutions which become exclusive.

2.2 The use and usefulness of personas in cybersecurity

Personas offer a solution to improving inclusive design for older adults. Indeed, personas were originally introduced as a practical way of better understanding end users, and considering them during the design of products and services [32]. Personas allow designers and developers the ability to understand how diverse users behave with a given context [6]; in this case, within a cybersecurity setting. Personas build on existing methods, such as scenarios, when seeking to identify the needs of specific user groups [54]. They have been in circulation within the academic community since their introduction by Cooper in the late 1990's [10], although the application of personas to cybersecurity has been limited, and even more so in older adult groups.

Stoll et al. [65] were the first to adapt personas to cybersecurity settings, creating three cybersecurity team members representing: an analyst, a safety officer and an intelligence researcher. They subsequently used these personas to inform the building of system architecture and 'consulted' the personas to ensure that their development was suitable. Mckenna et al. [63] also outlined how visual design methodologies could be applied to cybersecurity contexts. They highlighted the limitations of existing research, predominantly that the user is often only considered after the design of a solution is complete. Mckenna et al. produced personas representing: a cyber analyst, a network operations manager, a director of IT and a Chief Executive Officer (CEO) based on qualitative data gathered in relevant interviews and used these to inform design decisions. While both present early work in applying personas to cybersecurity, their work focuses entirely within workplace settings, and centres users with security expertise, a theme which is prevalent amongst the extant security literature.

In more recent years, the HCI community has moved towards more inclusive privacy and security – i.e., developing solutions which meet the needs of diverse user populations. Personas have also been used effectively in this regard. For example, Andrews [69] presents a number of personas which summarize the needs of a wide range of users including journalists, activists, members of the LGBTQI+ community and domestic violence survivors. Each of these groups, and many other groups, have specific needs for tools which protect their privacy and security, and as a result benefit from considering wider use cases than those which are immediately obvious. Older adults are no different in this regard, and designers and developers can benefit from understanding the variability in this population.

Despite this, very few personas exist which demonstrate the variability of the older adult population. Kim [26] used personas to understand how end users might become susceptible to security threats. Using a mixture of online surveys, articles and qualitative interviews, they developed eight personas reflecting distinct characteristics which contribute to cybersecurity vulnerability. Their personas consisted of four university students, two sets of married individuals with children, one user with very little demographic information (Responsive Rebecca) and one “elderly” woman (Innocent Irene). Innocent Irene is cast as: having extremely low awareness, making no effort to manage her personal information from cyber-attacks and relying on a tech store where she bought her devices. Kim et al. [26] highlight that their sample was predominantly based on younger users (aged 19-30), however, given that Innocent Irene is currently one of two older adult cybersecurity personas we have found in the entire literature base, it is clear that the diversity of older adult technology users is not appropriately reflected at present.

This paper sought to develop a set of dimensions from which older adult personas could be easily generated. The dimensions were drawn from recently published literature addressing various topics associated with older adult cybersecurity. Through identifying key dimensions associated with cybersecurity in this population, we produced two example older adult personas with various skillsets and priorities, each representing their own unique challenges for researchers, developers and policy makers. The dimensions we present can also be used to generate any number of new personas, each which is likely to represent a typology of older adults currently underserved in the technology space, although we present two here, for illustrative purposes.

3 METHOD

3.1 Selection Criteria

The current literature base focusing on older adult cybersecurity is relatively scarce, however, this paper builds on qualitative data from four recent studies addressing older adults’ cybersecurity resources, attitudes and behaviours. To motivate the design of the personas, we did an online literature search on the ACM Digital Library, Science Direct, and Google Scholar using the keywords [“older adults” OR “elderly” OR “seniors” AND “security” OR “cybersecurity”]. Then, we selected recently published articles that fit the following criteria: 1. Focusing on community-dwelling older adults/seniors/elderly (as self-defined by the paper), 2. Focusing on a cybersecurity context, and 3. Reported qualitative data. Four published papers met these search criteria. Original qualitative data from these four studies was provided and the combined raw data was subject to further analysis. This work was approved by our institution’s ethics review board.

3.2 Data Sources

All source studies included qualitative interviews lasting approximately one hour, with variability between 30 minutes and 120 minutes (see Table 1 for an overview of included studies). Interviews were for the most part conducted face to face, however, Study 4 (see below) reported using telephone interviews (as well as other surveying methods). The variability across these studies allowed us to consider older adult security behaviours across a broad range of contexts.

Table 1: Studies included in generating the dimensions.

Study	Ref	Year	Sample Data	Study Objectives
1	[45]	2021	*n* = 19 (F:8 M:4) older adults aged 62-78 (*m*=68.79)	Study 1 investigated OA's feelings towards cybersecurity and the barriers they face when doing so.
2	[49]	2019	*n* = 22 (F:15 M:7) older adults aged over 65 years old (*m*=72)	Study 2 investigated OA cybersecurity information support seeking behaviours including which factors are most important when seeking security support.
3	[46]	2020	*n* = (F:7 M:6) older adults aged 53-68 (*m*=63)	Study 3 investigated technological change in the retirement transition and its impact on cybersecurity behaviours and attitudes.
4	[50]	2021	*n* = 14 (F:5 M:9) older adults, aged between 55-80 years.	Study 4 was an intervention designed to train and embed security "guardians" within older adult communities.

3.3 Analysis

Data was combined and subjected to a template analysis [27]. A-priori themes taken from the four published papers provided a template for analysis, supplemented by other cybersecurity themes in the wider literature. Evidence for the relationship between the dimensions and behaviour has been found in the research literature, both in the studies used for this analysis and in the broader literature base, these are referred to explicitly within the analysis presented. Two personas were then created, which demonstrate two distinctly different users, generated by varying these dimensions. Each persona includes a variation on each of the dimensions (a cybersecurity profile) alongside a fictitious photograph; a set of demographics, and a description of the user, highlighting associated behaviours and attitudes.

4 RESULTS

Six a priori dimensions (themes) representing key characteristics likely to impact security behaviours in older adults were identified from within the data, as well as the broader, yet finite, cybersecurity literature base. These dimensions represent: *cybersecurity awareness*, *availability of support*, *digital literacy*, *stress*, *financial position* and *perceived responsibility for cybersecurity*. Each of these dimensions was identified as being a key factor in the ability of an older adult to protect themselves online, and the intersection of these dimensions provides unique challenges specific to older adults. Drawing from the security persona literature [26, 44, 69], we created a set of amalgamated personas based on these dimensions (and present two examples here). Prior to presenting the example personas, we outline each of the six key persona dimensions, as well as the existing literature which supports their importance.

4.1 Persona Dimensions

4.1.1Cybersecurity Awareness

Awareness is clearly an important concept, included in most core theories, frameworks and behavioural models of cybersecurity behaviour [18, 31]. Awareness is often the focus of human factors security interventions as well as a core facet of large-scale interventions and campaigns. Though not always successful in changing behaviour [3], awareness is necessary, but not independently sufficient to drive security behaviours [12].

Awareness of cybersecurity was highlighted Studies 2 and 4, where a lack of awareness leads to choosing poorer information sources, promoting vulnerability to threats. Existing literature has also identified awareness as an important factor for older adult cybersecurity vulnerability. Sannd [58] for example, investigated older adults' interactions with phishing emails and concluded that a lack of awareness, recognition ability, and poor treatment of phishing emails were likely to be key components of older adults remaining at high risk of phishing attacks. Similarly, Frik et al. [21] outlined how poor security awareness was associated with increased cybersecurity vulnerability in older adults living in care homes, with users only able to employ mitigation strategies when they had some awareness of security risks.

Although awareness is an important factor for older adult cybersecurity, not all older adults perform fewer cybersecurity behaviours than younger users. Parsons et al. [52] conducted a survey with 500 employees, 27% of which were over 51 years old. They found a positive relationship between age and information security behaviour, with older adults outperforming younger adults on the behavioural component of the HAIS-Q. Similarly, McCormac et al. [40] investigated individual differences and their association with information security awareness, finding that age was not significantly associated with awareness.

4.1.2Availability of Support

Asmar [2] outlined how support in the use of digital technologies is important for digital inclusion of older adults in online environments, and the quality and availability of this support is likely to influence an individual's cybersecurity vulnerability. Study 2 specifically set out to understand how older adults seek cybersecurity information. They found that older adults typically prioritize information sources based on their availability, rather than the level of expertise an individual can offer. Similarly, Study 1 found that older adults rely on technical support from others, but that this support is not always appropriate. Two distinct types of support were identified within Study 1 study. Firstly, support which promotes independence; this support was typically instructional advice, with family members showing the user how to do something, so that they could do it for themselves in the future. The second form of support identified was dependence promoting support. In these cases, support givers take the device from the older adult, complete the required tasks, and hand the device back. In these circumstances, the older adult is forced to rely on others to keep themselves secure, and do not develop their own security skillset. Study 3 also identified support as an important factor for recently retired individuals who have lost the support of younger colleagues and IT training upon retirement.

Outside of the three studies above, the current literature landscape is scarce relating to the impact of cybersecurity support on older adult cybersecurity. Mendel and Toch [42] highlighted that understanding older relations preferences is an important factor behind providing meaningful security and privacy support within family units. Murthy et al. [48] demonstrated that families living with older adults tend to have "self-appointed technology managers" who alternate between paternalism and stewardship in their attempts to keep older adults safe online. Security paternalism can also be seen in security practices of older adults receiving care, or those using health-monitoring systems, where assumptions around a lack of need for privacy are often made and acted upon [41, 43]. Finally, Kropcynski et al. [28] explored how communities of older adults work together to collectively manage their cybersecurity, finding that many older adults interacted with others with a similar level of technical expertise. Study 4 naturally builds on this study by training and embedding security guardians within their local communities to act as a source of support for older adults who without them would have none.

4.1.3Digital Literacy

Many definitions exist for digital literacy [55, 72], here we simplify digital literacy as ‘an individual’s ability to interact functionally with technology’. Many things are likely to feed into this, such as technological ability, device types as well as prior experience etc. Study 1 highlights that digital literacy is important for promoting confidence in an individual’s ability to engage in cybersecurity behaviours. Conversely, poor digital literacy leads users to unintentionally act in insecure ways, “burying their heads in the sand” and denying the existence of security threats. Study 2 highlights that digital literacy is necessary to interact effectively in the digital world, showing that information provided by security campaigns, etc., is only effective if users have the proper skillsets to make use of these resources. In Study 3, digital literacy was seen as important in allowing an individual to transition into retirement whilst counteracting the negative implications of losing workplace-based technical support.

Existing research has previously linked poor digital literacy with cybersecurity vulnerability. James et al. [24] outlined a relationship between digital literacy and susceptibility to scams in a large sample (*n*=639) of community-dwelling older adults. Lee [33] outlined the various ways in which a lack of digital literacy creates avenues for cybercrime victimization through increased susceptibility to phishing, as well as having decreased ability to identify and verify threats such as fake websites and social media accounts.

Digital literacy may lead to differences in how, and from whom, support is sought: an avenue for vulnerability in itself [50, 59]. It is also essential in allowing older adults to engage in technical cybersecurity practices: such as updating software, using antivirus programs, password managers or other technical solutions. Literacy levels are likely to impact the effectiveness of guidance and interventions by developers, policymakers and researchers, and along with the factors discussed above was seen as a key dimension.

4.1.4Stress

A growing body of literature is highlighting that cybersecurity can be an emotive subject for some users. Based in coping theory [30] and technostress [7] literature, D’Arcy [14] demonstrated how employees found information security requirements to be stressful. Study 1, which sought to understand how older adults felt about engaging in cybersecurity, outlined how the stress associated with cybersecurity could lead some older adults to disengage from security behaviours altogether. Similarly, some of the older adults interviewed in Study 3 identified that fear and anxiety around “doing the wrong thing” led them to rely heavily on others, even if the people they turned to were not necessarily experts. Fear, anxiety and a lack of confidence were also identified in Study 2 with users reporting avoidance of security advice found online in-case such advice was part of a larger cyber-attack.

A small but growing body of literature has demonstrated that stress and coping are important factors in cybersecurity. Decades of research entrenched in psychological models such as Protection Motivation Theory (PMT) [35] have often focused on threat appraisals, but more recently coping has gained traction as a better predictor of security behaviours [68, 70]. Given that the studies here, as well as other recent literature, have highlighted a growing importance of stress in cybersecurity, it was included as a key dimension here.

4.1.5Financial Position

An individual’s financial position is likely to impact their security environment in several ways. Access to technology has always been considered a component of the first level of the digital divide [57]. More recently, however, material access inequalities: those inequalities which stem from the variability in the quality of devices afforded to users of differing wealth status’ have become the focus of both security as well as digital inclusivity literatures [17, 23, 56]. Study 1 identified that some older adults see security protection as a waste of money. Similarly, Studies 2 and 3 reported users discussing how finances were too important to waste, and that following retirement, managing money became more important. The variability of financial position and its consequences for security was well outlined in the studies reviewed, however. Study 3 demonstrates that some older adults seek out paid help through local IT professionals, while Study 2 highlights that some users prefer to use free versions of anti-virus software to avoid spending money unnecessarily. Study 3 also highlighted how a lack of wealth might lead some users to use hand-me-down devices which might be outdated and be more vulnerable to cyber-attacks.

4.1.6Perceived Responsibility for Security

The final dimension outlined as important for older adult cybersecurity was the level of responsibility that people feel in relation to their cybersecurity. Study 1 demonstrated that users can sometimes defer the responsibility of cybersecurity to others for reasons of stress, fear and anxiety, as discussed above. Often users simply do not feel comfortable enough to engage in security, fearing that they will cause further issues. Others feel that organizations and retailers have a duty of care to provide ongoing effective security support for devices so that consumers are protected, although in reality this thought process is unlikely to help against many forms of social engineering-based attacks such as phishing. Study 4 demonstrated the positive effects of empowering users with a sense of responsibility for cybersecurity education, although this represents an extreme case, as most users will not have access to specific cybersecurity training. However, it does demonstrate a link between ownership and security salience.

Whether or not security is, or should be, a personal responsibility is a matter of debate. Some believe that attributing security to personal responsibility risks producing an environment where victim shaming becomes the norm, as outlined in the interesting discussion of this topic by Strawser and Joy [66]. Conversely, LaRose [29] found that those who agreed with the statement that “online safety is my personal responsibility” were significantly more likely to protect themselves online than those who disagreed, though they acknowledge that causation could not be implied through such survey studies. Interestingly LaRose found that an exception to the trend was identified when users reported low self-efficacy. These users demonstrated even lower security intentions after being told that safety was their responsibility, suggesting that having responsibility thrust upon them was discouraging. This finding aligns with the above-mentioned stress reaction to security and is likely to be rife in users with low digital literacy.

4.1.7Interactions between the dimensions

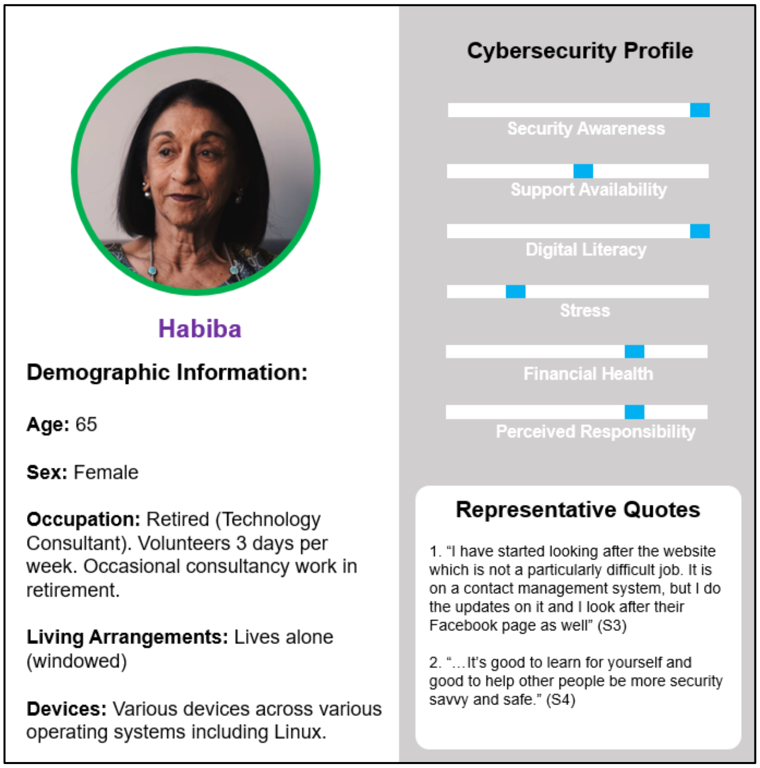
Although the dimensions above are outlined individually it is likely that there will be considerable interplay between the above dimensions. For example, users with higher digital literacy may experience less stress when seeking to navigate cybersecurity protection. Alternatively, those with greater financial wellbeing may be less interested in taking responsibility for their cybersecurity if they can delegate this responsibility to a paid other. Of course, both situations can be reversed, with more affluent users taking more responsibility for cybersecurity, as they have more to lose, and users with greater digital literacy being more aware of various security threats, giving a higher stress response. Both circumstances are likely to exist, and both are likely to need tailored solutions.

4.2 Introducing Older Adult Cybersecurity Personas

Any number of personas can be generated by manipulating the six dimensions described above and we give two examples below. Representative quotes were provided for each of the personas, taken verbatim or slightly adapted from the source studies discussed throughout this paper, lending evidence to the sorts of quotes that might be provided by these users. A quote from Study 1 is listed as S1 etc. Facial images attached to the personas were taken with consent from https://unsplash.com.

4.2.1Persona 1: Habiba

Habiba spent the latter part of her career as a technology consultant, after working as a developer during the earliest iterations of household computing technology. She has incredibly high digital literacy and is very aware of cybersecurity threats as well as how she can protect herself from them. Habiba is continually frustrated when she sees stereotypes of older users and finds almost all security messages targeted at older adults condescending.



Habiba

Demographic Information:

Age: 65

Sex: Female

Occupation: Retired (Technology Consultant). Volunteers 3 days per week. Occasional consultancy work in retirement.

Living Arrangements: Lives alone (windowed)

Devices: Various devices across various operating systems including Linux.

Cybersecurity Profile

Representative Quotes

1. "I have started looking after the website which is not a particularly difficult job. It is on a contact management system, but I do the updates on it and I look after their Facebook page as well" (S3)

2. "…It's good to learn for yourself and good to help other people be more security savvy and safe." (S4)

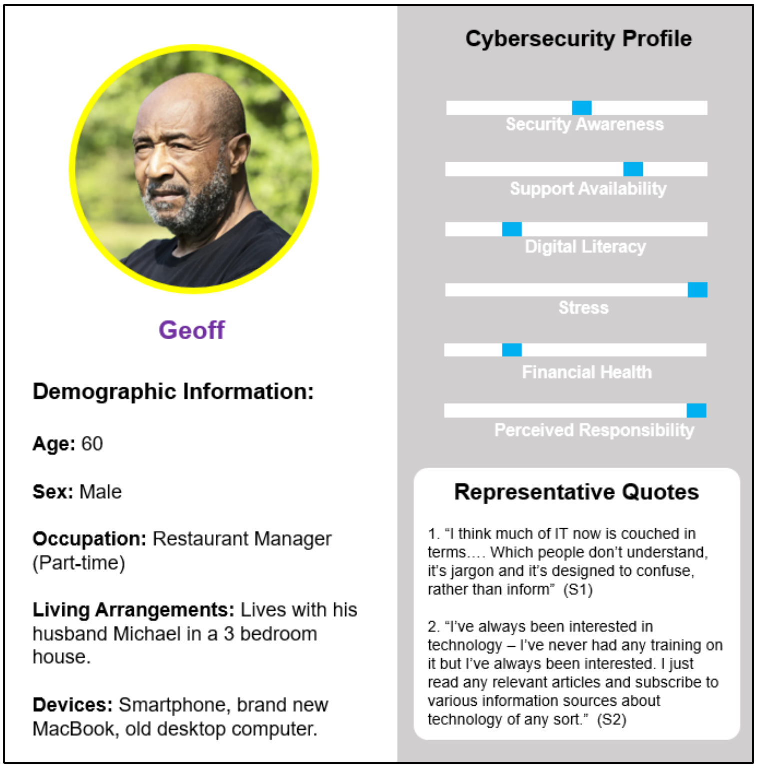
Although she has now retired, Habiba occasionally takes on consultancy work for fun. She notes how this also helps keep her knowledge up to date. She volunteers 3 days per week across two roles; one with a local charity, where having been identified as being technologically literate, she was given the role of running accounting and financial software packages, as well as taking control of cybersecurity. In her second role, she provides technical support for other older adults as part of a coffee meet at her local IT shop.

Habiba describes her technology usage as "non-stop", with IoT devices scattered around her home including Hive heating, a camera doorbell, and even a Wi-Fi enabled kettle. Habiba keeps her devices up to date and buys new devices when software is no longer supported. She is an early adopter of security solutions such as password managers, and believes that people should take responsibility for their cybersecurity.

Although Habiba lives alone, she is not worried about lacking support from others, as she is confident that she "couldn't be any more secure". On rare occasions where Habiba does not know the answer, she feels more than comfortable engaging in technology forums such as GitHub to find the answers she needs.

4.2.2Persona 2: Geoff

Geoff's husband Michael recently purchased him a new MacBook for his 60th birthday. The Apple Genius Bar set the device up for him and he is continually delighted by how simple it is to use compared to other devices he has had in the past. Geoff uses his laptop for managing his work activities such as creating staff rotas, but also enjoys leisure activities such as watching Netflix. Geoff finds cybersecurity to be incredibly stressful because he feels like he knows nothing about it. Although keen to use technology, Geoff has always struggled with jargon around cybersecurity. Michael is similarly confused by cybersecurity, but finds the topic less than interesting, believing that there are better things to do than spending time reading about back-ups. Geoff usually still asks Michael for help anyway, however, Michael usually 'presses random buttons until it works'. Although Geoff would love to use the Genius Bar, it is too far from where they live, so is used in emergencies only.


Cybersecurity Profile
Security Awareness
Support Availability
Digital Literacy
Stress
Financial Health
Perceived Responsibility

Geoff

Demographic Information:

Age: 60

Sex: Male

Occupation: Restaurant Manager (Part-time)

Living Arrangements: Lives with his husband Michael in a 3 bedroom house.

Devices: Smartphone, brand new MacBook, old desktop computer.

Representative Quotes

1. "I think much of IT now is couched in terms…. Which people don't understand, it's jargon and it's designed to confuse, rather than inform" (S1)

2. "I've always been interested in technology – I've never had any training on it but I've always been interested. I just read any relevant articles and subscribe to various information sources about technology of any sort." (S2)

Geoff is aware that his cybersecurity hygiene could be better but takes physical measures to try to mitigate this. For example, he hides his devices before leaving the house, since the devices are not secured with passwords. He writes down login details, something he thinks is risky, but feels he has to do this as he can never remember passwords. When banking online, he tends to use his old desktop PC over his new MacBook, since it "just feels safer". Geoff has little money to spare, so refuses to purchase anti-virus software, instead relying on free versions. He has considered purchasing software but is unsure about which features he needs, as many are pushed by his program, and wonders if they are necessary at all. Geoff wants to take control of his cybersecurity but feels that there is far too little support available.

5 GENERAL DISCUSSION

This paper set out to produce a means to generate fictional architypes of older adults based on recent qualitative research investigating various aspects of older adult cybersecurity, highlighting important dimensions which are likely to influence older adult cybersecurity behaviours and subsequent vulnerability. These dimensions are: *security awareness*, *support availability*, *digital literacy*, *stress*, *financial health* and *perceived responsibility*.

Too often older adults are represented as a homogenous population with a collective set of needs [20] and while personas have been developed for privacy and security purposes [19, 26], very little existing literature has considered older adults within this persona development. However, this population is as diverse as any other, something we hope is demonstrated by the example personas developed within this paper. The personas offered here serve as just two representations of a vast number of older adult users, who are likely to vary drastically on the dimensions outlined here. We hope that outlining this variability will help designers and developers to consider older adults as a more diverse user group, whilst also providing researchers a starting point for developing future research agendas.

5.1 Thinking More Broadly About Older Adults' Cybersecurity

The dimensions outlined in this paper are proposed as salient starting points when thinking about designing security interventions or tools for older adults in order to counteract pre-existing stereotypes of older adult users. For example, we can easily see how very basic security advice tailored to those with very low digital literacy would be: ignored, unsuitable for, or perhaps even offensive to users such as Habiba. Similarly, paid-for security solutions which might be seen as acceptable and feasible by some older adults, may deter users such as Geoff, who simply cannot justify the costs, given their limited financial position. Advice reminding older adults to update their devices, even if understood by those with the appropriate levels of literacy, and even if considered not to be stressful enough to scare users away, may be entirely inappropriate to users who rely on hand-me-down devices, which are so outdated that they are no longer supported by security updates. Users such as Geoff, who experience high levels of stress around security may be best served by solutions which promote self-efficacy and technology use, rather than high-fear messages reminding users of the multitude of threats online [3]. In this paper, we present a more diverse sample of older adults to discourage the notion that the older adult population can be condensed down to broad, stereotypical representations. Of course, it is important to emphasize that the dimensions listed here are not necessarily exhaustive and should be updated as new and relevant literature emerges.

5.2 Limitations

Although we present a range of dimensions relevant for the design of cybersecurity interventions and tools for older adults, others are also likely to exist. The focus of older users in the field of cybersecurity is a relatively recent approach, and as such this work was based on a finite amount of recent qualitative research. This qualitative work is well positioned to provide rich discourse about the dimensions outlined here but would benefit from quantitative research designed to determine how these dimensions impact older adult security vulnerability in statistically significant ways. Similarly, identifying meaningful interactions between these dimensions, as discussed above, would be useful for designing interventions and solutions for older adults.

Another consideration in this paper is the diversity of the participants underpinning the data. Since the personas generated here are derived directly from data captured in recent qualitative studies discussed. The dimensions ultimately reflect the populations sampled within those papers. Given the small samples associated with qualitative research, representativeness is not possible, nor typically sought after, but we identify that further work needs to be done to understand the issues experienced by those older adults who do not necessarily sit in those groups which are most represented in research.

6 CONCLUSION

In this paper we have constructed and described an evidence-based means to generate personas representing a varied set of older adult technology users. We have drawn upon recent existing qualitative cybersecurity research conducted with older adult samples to identify key characteristics likely to influence older adult security behaviours: Security Awareness, Support Available, Digital Literacy, Stress, Financial Health, and Perceived Responsibility. We have then used these six dimensions to develop two illustrative personas to demonstrate some of the variability within this population, and to aid in the design of security interventions and tools.

7 REFERENCES

[1] Age-UK 2015. Over half of people aged 65 + targeted by fraudsters. *Age UK*. April 2015 (2015), 2015–2017.

[2] Asmar, A. et al. 2020. Social support for digital inclusion: Towards a typology of social support patterns. *Social Inclusion*. 8, 2 (2020), 138–150. DOI:https://doi.org/10.17645/si.v8i2.2627.

[3] Bada, M. et al. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

[4] Birkland, J.L.H. 2019. *Gerontechnology: understanding older adult information and communication technology use*. Emerald Publishing Limited.

[5] Blanco, T. et al. 2017. Deconstructing the Tower of Babel: a design method to improve empathy and teamwork competences of informatics students. *International Journal of Technology and Design Education*. 27, 2 (2017), 307–328. DOI:https://doi.org/10.1007/s10798-015-9348-6.

[6] Briggs, P. et al. 2012. Invisible design: Exploring insights and ideas through ambiguous film scenarios. *Proceedings of the Designing Interactive Systems Conference, DIS '12*. June (2012), 534–543. DOI:https://doi.org/10.1145/2317956.2318036.

[7] Chiappetta, M. 2017. The Technostress: definition, symptoms and risk prevention. *Senses Sci*. 4, 1 (2017), 358–361. DOI:https://doi.org/10.14616/sands-2017-1-358361.

[8] Chiu, C.J. and Liu, C.W. 2017. Understanding Older Adult's Technology Adoption and Withdrawal for Elderly Care and Education: Mixed Method Analysis from National Survey. *Journal of Medical Internet Research*. 19, 11 (2017), e374. DOI:https://doi.org/10.2196/jmir.7401.

[9] Chiu, C.J. and Liu, C.W. 2017. Understanding older adult's technology adoption and withdrawal for elderly care and education: Mixed method analysis from national survey.

Journal of Medical Internet Research. 19, 11 (2017), 1–11. DOI:https://doi.org/10.2196/jmir.7401.

[10] Cooper, A. 1999. The Inmates are Running the Asylum. 17–17.

[11] Cosco, T.D. et al. 2021. Covid-19, social isolation, and mental health among older adults:a digital catch-22. *Journal of Medical Internet Research*. 23, 5 (2021), 22–24. DOI:https://doi.org/10.2196/21864.

[12] Coventry, L. et al. 2014. Using behavioural insights to improve the public ' s use of cyber security best practices improve the public ' s use of cyber. *Project Report. Government Office for Science*. (2014), 1–20.

[13] Damodaran, L. and Sandhu, J. 2016. The role of a social context for ICT learning and support in reducing digital inequalities for older ICT users. *International Journal of Learning Technology*. 11, 2 (2016), 1–20. DOI:https://doi.org/10.1504/IJLT.2016.077520.

[14] D'Arcy, J. et al. 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*. 31, 2 (2014), 285–318. DOI:https://doi.org/10.2753/MIS0742-1222310210.

[15] Demographics of Internet and Home Broadband Usage in the United States: 2021. *https://www.pewresearch.org/internet/fact-sheet/internet-broadband/?menuItem=9a15d0d3-3bff-4e9e-a329-6e328bc7bcce*. Accessed: 2021-09-08.

[16] Derynda, B. et al. 2020. Technology Adoption Among Seniors During COVID-19 Pandemic Impacts Mental Health and Feelings of Companionship. *Innovation in Aging*. 4, Supplement_1 (Dec. 2020), 965–965. DOI:https://doi.org/10.1093/geroni/igaa057.3526.

[17] van Deursen, A.J.A.M. and van Dijk, J.A.G.M. 2019. The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *New Media and Society*. 21, 2 (2019), 354–375. DOI:https://doi.org/10.1177/1461444818797082.

[18] Dinev, T. and Hu, Q. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*. 8, 7 (2007), 386–408. DOI:https://doi.org/10.17705/1jais.00133.

[19] Dupree, J.L. et al. 2016. Privacy personas: Clustering users via attitudes and behaviors toward security practices. *Conference on Human Factors in Computing Systems - Proceedings*. (2016), 5228–5239. DOI:https://doi.org/10.1145/2858036.2858214.

[20] Friemel, T.N. 2016. The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*. 18, 2 (Feb. 2016), 313–331. DOI:https://doi.org/10.1177/1461444814538648.

[21] Frik, A. et al. 2019. Privacy and security threat models and mitigation strategies of older adults. *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*. (2019), 21–40.

[22] Haase, K.R. et al. 2021. Older adults' experiences with using technology for socialization during the COVID-19 pandemic: Cross-sectional survey study. *JMIR Aging*. 4, 2 (2021). DOI:https://doi.org/10.2196/28010.

[23] Helsper, E.J. and Reisdorf, B.C. 2017. The emergence of a “digital underclass” in Great Britain and Sweden: Changing reasons for digital exclusion. *New Media and Society*. 19, 8 (2017), 1253–1270. DOI:https://doi.org/10.1177/1461444816634676.

[24] James, B.D. et al. 2014. Correlates of Susceptibility to Scams in Older Adults Without Dementia. *Journal of Elder Abuse and Neglect*. 26, 2 (Mar. 2014), 107–122. DOI:https://doi.org/10.1080/08946566.2013.821809.

[25] Karaoglu, G. et al. 2021. Changing Technologies , Changing Lives : Older Adults ’ Perspectives on the Benefits of Using New Technologies. 15, (2021), 3887–3907.

[26] Kim, E. et al. 2019. From innocent irene to parental patrick: Framing user characteristics and personas to design for cybersecurity. *Proceedings of the International Conference on Engineering Design, ICED*. 2019-Augus, AUGUST (2019), 1773–1782. DOI:https://doi.org/10.1017/dsi.2019.183.

[27] King 1998. Template analysis. *Qualitative methods and analysis in organizational research: A practical guide.* Sage Publications Ltd. 118–134.

[28] Kropczynski, J. et al. 2021. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Proceedings of the ACM on Human-Computer Interaction*. 4, CSCW3 (2021), 1–27. DOI:https://doi.org/10.1145/3432954.

[29] LaRose, R. et al. 2008. Promoting personal responsibility for internet safety. *Communications of the ACM*. 51, 3 (2008), 71–76. DOI:https://doi.org/10.1145/1325555.1325569.

[30] Lazarus, R.S. and DeLongis, A. 1983. Psychological stress and coping in aging. *American Psychologist*. 38, 3 (1983), 245–254. DOI:https://doi.org/10.1037/0003-066X.38.3.245.

[31] Lebek, B. et al. 2014. Information security awareness and behavior: A theory-based literature review. *Management Research Review*. 37, 12 (2014), 1049–1092. DOI:https://doi.org/10.1108/MRR-04-2013-0085.

[32] Lee, M. et al. 2020. Developing personas & use cases with user survey data: A study on the millennials’ media usage. *Journal of Retailing and Consumer Services*. 54, June 2019 (2020), 102051. DOI:https://doi.org/10.1016/j.jretconser.2020.102051.

[33] Lee, N.M. 2018. Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom. *Communication Education*. 67, 4 (2018), 460–466. DOI:https://doi.org/10.1080/03634523.2018.1503313.

[34] LexisNexis 2021. *Fraud - The Facts*.

[35] Maddux, J.E. and Rogers, R.W. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*. 19, 5 (1983), 469–479. DOI:https://doi.org/10.1016/0022-1031(83)90023-9.

[36] Mariano, J. et al. 2022. Too old for technology? Stereotype threat and technology use by older adults. *Behaviour & Information Technology*. 41, 7 (May 2022), 1503–1514. DOI:https://doi.org/10.1080/0144929X.2021.1882577.

[37] Mariano, J. et al. 2021. Too old for technology? Stereotype threat and technology use by older adults. *Behaviour and Information Technology*. (2021). DOI:https://doi.org/10.1080/0144929X.2021.1882577.

[38] Marques, S. et al. 2020. Determinants of ageism against older adults: A systematic review. *International Journal of Environmental Research and Public Health*. 17, 7 (2020). DOI:https://doi.org/10.3390/ijerph17072560.

[39] Marston, H.R. et al. 2019. Older Adults' Perceptions of ICT: Main Findings from the Technology In Later Life (TILL) Study. *Healthcare*. 7, 3 (Jul. 2019), 86. DOI:https://doi.org/10.3390/healthcare7030086.

[40] McCormac, A. et al. 2017. Individual differences and Information Security Awareness. *Computers in Human Behavior*. 69, (2017), 151–156. DOI:https://doi.org/10.1016/j.chb.2016.11.065.

[41] McNeill, A. et al. 2017. Functional privacy concerns of older adults about pervasive health-monitoring systems. *ACM International Conference Proceeding Series*. Part F1285, (2017), 96–102. DOI:https://doi.org/10.1145/3056540.3056559.

[42] Mendel, T. and Toch, E. 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). DOI:https://doi.org/10.1145/3369821.

[43] Mentis, H.M. et al. 2019. Upside and downside risk in online security for older adults with mild cognitive impairment. *Conference on Human Factors in Computing Systems - Proceedings*. (2019), 1–13. DOI:https://doi.org/10.1145/3290605.3300573.

[44] Miaskiewicz, T. and Kozar, K.A. 2011. Personas and user-centered design: How can personas benefit product design processes? *Design Studies*. 32, 5 (2011), 417–430. DOI:https://doi.org/10.1016/j.destud.2011.03.003.

[45] Morrison, B. et al. 2021. How do Older Adults feel about engaging with Cyber-Security? *Human Behavior and Emerging Technologies*. 3, 5 (2021), 1033–1049. DOI:https://doi.org/10.1002/hbe2.291.

[46] Morrison, B.A. et al. 2020. Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults. *Frontiers in Psychology*. 11, April (2020), 1–13. DOI:https://doi.org/10.3389/fpsyg.2020.00623.

[47] Munanga, A. 2019. A New and Growing Problem for Older Adults. (2019), 2017–2020.

[48] Murthy, S. et al. 2021. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. 5, April (2021), 1–24.

[49] Nicholson, J. et al. 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 February (2019). DOI:https://doi.org/10.1145/3290605.3300579.

[50] Nicholson, J. and McGlasson, J. 2020. CyberGuardians: Improving community cyber resilience through embedded peer-to-peer support. *DIS 2020 Companion - Companion Publication of the 2020 ACM Designing Interactive Systems Conference*. (2020), 117–121. DOI:https://doi.org/10.1145/3393914.3395871.

[51] Office for National Statistics 2019. Exploring the UK s digital divide.pdf. March (2019).

[52] Parsons, K. et al. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*. 42, (2014), 165–176. DOI:https://doi.org/10.1016/j.cose.2013.12.003.

[53] Petrie, H. 2023. Talking ‘bout my Generation … or not?: The Digital Technology Life Experiences of Older People. *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg Germany, Apr. 2023), 1–9.

[54] Pruitt, J. and Grudin, J. 2003. Personas: Practice and Theory. *Proceedings of the 2003 conference on Designing for user experiences - DUX ’03* (New York, New York, USA, 2003), 1.

[55] Radovanović, D. et al. 2020. Digital literacy key performance indicators for sustainable development. *Social Inclusion*. 8, 2 (2020), 151–167. DOI:https://doi.org/10.17645/si.v8i2.2587.

[56] Reisdorf, B. and Rhinesmith, C. 2020. Digital inclusion as a core component of social inclusion. *Social Inclusion*. 8, 2 (2020), 132–137. DOI:https://doi.org/10.17645/si.v8i2.3184.

[57] Robinson, L. et al. 2015. Digital inequalities and why they matter. *Information Communication and Society*. 18, 5 (2015), 569–582. DOI:https://doi.org/10.1080/1369118X.2015.1012532.

[58] Sannd, P. and Cook, D.M. 2018. Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks. *14th International Conference on Information Processing: Internet of Things, ICInPro 2018 - Proceedings*. (2018). DOI:https://doi.org/10.1109/ICINPRO43533.2018.9096878.

[59] Schreurs, K. et al. 2017. Problematizing the Digital Literacy Paradox in the Context of Older Adults’ ICT Use: Aging, Media Discourse, and Self-Determination. *Canadian Journal of Communication*. 42, 2 (2017), 359–377. DOI:https://doi.org/10.22230/cjc.2017v42n2a3130.

[60] Schulz, R. et al. 2015. Advancing the aging and technology agenda in gerontology. *Gerontologist*. 55, 5 (2015), 724–734. DOI:https://doi.org/10.1093/geront/gnu071.

[61] Seifert, A. 2020. The Digital Exclusion of Older Adults during the COVID-19 Pandemic. *Journal of Gerontological Social Work*. 00, 00 (2020), 1–3. DOI:https://doi.org/10.1080/01634372.2020.1764687.

[62] Shao, J. et al. 2019. Why are older adults victims of fraud? Current knowledge and prospects regarding older adults’ vulnerability to fraud. *Journal of Elder Abuse and Neglect*. 31, 3 (2019), 225–243. DOI:https://doi.org/10.1080/08946566.2019.1625842.

[63] Staheli, D. et al. 2014. Visualization evaluation for cyber security. (2014), 49–56. DOI:https://doi.org/10.1145/2671491.2671492.

[64] Stephens, C. et al. 2015. Volunteering as reciprocity: Beneficial and harmful effects of social policies to encourage contribution in older age. *Journal of Aging Studies*. 33, (2015), 22–27. DOI:https://doi.org/10.1016/j.jaging.2015.02.003.

[65] Stoll, J. et al. 2008. Adapting personas for use in security visualization design. *Mathematics and Visualization*. (2008), 39–52. DOI:https://doi.org/10.1007/978-3-540-78243-8_3.

[66] Strawser, B.J. and Joy, D.J. 2015. Cyber Security and User Responsibility: Surprising Normative Differences. *Procedia Manufacturing*. 3, Ahfe (2015), 1101–1108. DOI:https://doi.org/10.1016/j.promfg.2015.07.183.

[67] Todd D. Nelson 2005. Ageism: Prejudice against our feared future self. *Journal of Social Issues*. 61, 2 (2005), 207–221.

[68] Tsai, H.S. et al. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*. 59, (Jun. 2016), 138–150. DOI:https://doi.org/10.1016/j.cose.2016.02.009.

[69] User Personas for Privacy and Security: 2015. .

[70] Van Bavel, R. et al. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*. 123, (Mar. 2019), 29–39. DOI:https://doi.org/10.1016/j.ijhcs.2018.11.003.

[71] Vines, J. et al. 2015. An Age-Old Problem : Examining the Discourses of Ageing in HCI and Strategies for Future Research. *Tochi*. 22, 1 (2015), 1–27. DOI:https://doi.org/10.1145/2696867.

[72] Vuorikari, R. et al. 2016. DigComp 2.0 - The Digital Competence Framework for Citizens.