“It’s the one thing that makes my life tick”: Security Perspectives of the Smartphone Era

Matt Dixon
Pact Lab, Northumbria University, United Kingdom, matt2.dixon@northumbria.ac.uk

Elizabeth Sillence
Pact Lab, Northumbria University, United Kingdom, elizabeth.sillence@northumbria.ac.uk

James Nicholson
Department of Computer and Information Science, Northumbria University, United Kingdom, james.nicholson@northumbria.ac.uk

Lynne Coventry
Division of Cybersecurity, Abertay University, United Kingdom, l.coventry@abertay.ac.uk

As smartphones overtake personal computers as the device of choice for internet access and everyday digital tasks, cybersecurity becomes a pressing issue for the platform. Research has found that smartphone users appear to act less securely than they would on a PC, but the reasons for this are unclear. The technology, the threats, and the role of smartphones have all developed in recent years, and this paper examines what smartphone security looks like to users in the 2020s. We interviewed 27 smartphone users about their security attitudes and behaviours. We find that users place great emphasis on, and take responsibility for, the physical security of their device, but minimise their responsibility for dealing with digital threats. We observe key contextual factors that influence how users protect their smartphones. The increasing monetary cost of smartphones and users’ functional reliance on them, causes participants to be highly concerned with protecting the physical safety and integrity of their devices. However, users appear to have a high level of trust in apps, based on the vetting processes of official app stores, yet they are still vulnerable to abuse from malicious/unnecessary permissions, and exhibit poor security habits when accessing illegitimate, pirated media outside of their smartphone’s app store.

CCS CONCEPTS •Security and privacy•Human-centered computing~Ubiquitous and mobile computing~Ubiquitous and mobile devices~Smartphones

Additional Keywords and Phrases: Smartphones, Security and Privacy, Extended Self

ACM Reference Format:

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

1 Introduction

Smartphones are a defining technology of the 21st century following a remarkable boom in the last ten years. The vast influence of the smartphone can be observed in many ways, including the widespread ownership of smartphones across the world. A worldwide report of smartphone ownership [53] found that in advanced economies, 76% of all adults own a smartphone on average. Ownership is likely to continue growing globally as the two core groups of non-adopters; older adults and adults in developing economies, continue to increase their uptake [53]. However, the influence of smartphones goes beyond simple ownership. From as early as 2015 major regulators have labelled countries such as the UK as a ‘Smartphone Society’ [41] defined by the population’s preference for internet access shifting to smartphones from laptop or desktop computers (collectively referred to as ‘PCs’ from here on). This shift has progressed so much that some internet users do not own or use a PC, and perceive a smartphone as sufficient to meet their online needs [42].

Alongside the rise in the smartphone’s popularity, security threats targeting these devices have also seen a significant rise, with attacks doubling between 2017 and 2018 to over 116.5 million [54]. 2021 also saw the rise of powerful, government operated spyware known as ‘Pegasus’, which became known to the public after significant media coverage. Extensive journalistic investigations [55] found that phones belonging to activists, journalists and politicians had been affected by the malware which gives root access to the attacker. While Pegasus is unlikely to be used against the average user, security researchers continue to identify malware threats that target average users, such as ‘trojanised’ apps, which offer a legitimate function, but begin to act maliciously against users [5]. Such malware is highly lucrative in terms of data acquisition, as smartphone users store more personal data on their smartphones than their computers [12]. This is problematic, as prior research has highlighted how smartphone users use security applications (e.g., anti-malware) significantly less often than on a PC [3, 12, 51]. With smartphones becoming so central to modern life, understanding how

and why users protect their devices will help identify where they may be vulnerable, and where the smartphone system and/or user awareness can be improved.

Research has focused on various human aspects of smartphone cybersecurity, sometimes in a broad sense, capturing perspectives across a range of security issues, e.g., [15, 56] and addressing specific areas of concern, such as attitudes to locking mechanisms [20, 25, 26, 31], privacy and security settings [21], threat awareness [32, 40] and unauthorised access [34, 39]. However, many aspects of this work can quickly become outdated due to the pace at which the technology, and its usage context, evolves. We aim to provide a timely refresh to our understanding of user perspectives, with a strong focus on the context of the smartphone as a central platform for handling personal organisation, work, study, recreation, socialisation and more.

This study contributes the following:

- An exploration of user perceptions of smartphone security, refreshing findings from prior work such as Chin et al. 2012 [15].
- Contextual insights as to how user perceptions have evolved; particularly why the same overarching threats remain prevalent, but how these target different values of smartphone users.
- Insights into where users focus their responsibility (physical security), and where their protective behaviours may be lacking (e.g., poor permission management, and lax privacy control).
- Identification of an underexplored risky behaviour carried out on smartphones; downloading of pirated media, coupled with a lack of protective behaviours that users would usually engage with on a PC platform, but fail to carry over to their smartphone.

2 Background literature

2.1 User perceptions and experiences of smartphone security and privacy

Some notable works have approached privacy and security from a broad standpoint, aiming to explore perceptions and measure security behaviours as a whole, rather than investigating specific security behaviours. One key example of such work is [15]. Their mixed methods study compares smartphones to PCs, surveying users to assess how comfortable they feel when engaging with various sensitive tasks, including mobile banking, online shopping, or tasks involving private data, such as a Social Security Number. They found users to be typically less trusting of their smartphones for sensitive tasks but take a riskier attitude to installing apps on their smartphones, with little care for security indicators, instead relying on user reviews and recommendations to establish trust. In the years since this study, these sensitive tasks have become highly commonplace on mobile phones; 73% of e-commerce sales stem from mobile devices [37], 80% of adults in the UK use mobile banking [24] and globally, researchers have documented the digitization of state services driving many more individuals to carry out sensitive tasks involving personal data on mobile devices [36].

A more recent survey by Thompson and McGill [56], compares smartphones to PCs, comparing the day-to-day activities and security behaviours engaged with on each platform. They also measure user perceptions of security through Protection Motivation Theory (PMT) constructs [45] and Self Efficacy [7]. Their findings indicate that users typically act less securely on their smartphones, for example performing less frequent data backups, software updates, antivirus scans, or protecting the device with a password. However, at the time of this work, more sensitive tasks were still carried out on PCs than smartphones [41] unlike today. New research is required to ascertain whether the recent shift in platform preference, is accompanied by improved security behaviours.

Below, we discuss further work in the field of smartphone security and privacy, dividing work into two categories: first, research on physical security, such as locking behaviours and unauthorized access and second, research focusing on digital threats such as malware, and the legitimacy of apps.

2.2 Authentication, locking and unauthorized access

Early work such as [8] investigates the security needs of users, finding that users carried out sensitive tasks and stored sensitive data on their smartphones, yet perceived Personal Identifiable Number (PIN) locks (the only widely available locking mechanisms at the time) as ineffective protection. Further work, such as [20] focuses on how often users choose to employ a locking mechanism, and their motivations for doing (or not doing) so. They found that only 58% of smartphone users used a locking mechanism, with qualitative findings indicating that locking was perceived as inconvenient, or not necessary for the data on their phone. Further research explored the perception of smartphone locks in practice [26], using a field study to investigate, finding that typically 3% of smartphone time was dedicated to unlocking – up to 9% in the worst case. They also looked at the perception of locking at specific instances; 24% of authentication instances were considered to be unnecessary (typically as they were at home), suggesting inconvenience may be a significant factor in deterring users from utilizing screen locks.

As smartphone technology developed, biometrics such as fingerprint scans and face recognition became available. Biometrics were sold as reducing the inconvenience factor of unlocking the smartphone by offering quicker, less effortful authentication. Research on these authentication methods [31] indicates that fingerprint scans were perceived to be more usable than face recognition by users. Face recognition had a higher rate of failure (thus more inconvenient), and was viewed as 'socially incompatible', with users claiming they 'felt like they were taking selfies all day', making them self-

conscious in public settings. However, given that this study was conducted while biometrics were a new addition to smartphones, the technology has likely advanced to reduce failure rates, and minimise the need to carefully position the phone to capture the face.

Further research has focused on 'implicit authentication' in which authentication requirements are disabled when the device is believed to be securely with its owner, for example, based on its location. An existing service which makes use of implicit authentication is Google's Smart Lock, where the user can indicate secure locations such as their home, where their locking mechanisms will be disabled. A study on this particular service indicates that users find the benefits of the Smart Lock to be unclear and view it as a security concern [35], suggesting users do sometimes feel a lock is necessary even in the safety of their own home. This aligns with wider findings that indicate known-persons, often with a close relationship to the victim, to be a significant risk factor in smartphone security, equivalent to "insider threats" faced by organisations [26, 33, 34, 39]. These 'insider' attacks against smartphones can be highly successful, typically due to knowledge of an unlock code, perhaps explicitly shared by the owner as an expression of trust or having multiple chances to surreptitiously observe the owner when entering it. Unauthorized access in such contexts do constitute a security breach, but also a breach of personal privacy. The aims of insiders range from snooping on message history, internet browsing history and locations but can extend to installing malware or spyware or even stealing money via banking or other finance apps. Snooping, or installation of software that allows the attacker to monitor the victim may also occur in situations of domestic abuse, in which perpetrators aim to control and monitor the victim using their smartphone, potentially without their knowledge [14].

2.3 Digital threats; apps, malware, and network security

App selection, and assessment of an app's trustworthiness, has received much research attention. Chin et al.'s [15] findings indicate that users typically find new apps by browsing, or from recommendations from friends, and make installation choices without properly evaluating the source of the app or any security indicators provided by the platform. The use of security apps is also of great interest, as these appear to be majorly under-utilized by smartphone users. Breitinger et. al. measure how users engage with security software and settings, finding that despite storing more personal data on smartphones than PCs, users are less likely to install security software on their smartphone, such as an anti-virus or Virtual Private Network (VPN) [12]. This was true even for self-rated 'expert' smartphone users. The uptake of third-party security software remains unclear, with some studies recording uptake as low as 29% [32], or only as high as 57% [29].

Breitinger et al. also explored differences between users of Android and iOS, finding that Android users were typically more security conscious, and more likely to explore and customize security settings [12], a finding which has been corroborated by other studies, e.g. iOS tended to be more popular amongst users who reported weaker security knowledge [44].

Watson & Zheng [58] reviewed literature to create a list of smartphone security behaviours recommended by security research, and surveyed how smartphone users engaged with these behaviours. They found that users, particularly those without IT training, did not engage with several critical security behaviours identified in their review, such as encrypting files on their device or enabling remote security features and other anti-theft measures. Similarly, [21] found that users were widely unaware of the security features and configurations available to them, as well as held incorrect beliefs about the risks their smartphone face, and how different security settings may (or may not) protect them. They found that the low levels of engagement with security settings and features was due to a perception that security settings would be too complex and effortful to navigate, and not effective.

The use of unsecured Wi-Fi networks may also be problematic. Alsaleh, Alomar & Alarifi [3] indicate that users are widely unaware of the risks of such use, with only 30% of their sample aware of risks associated with public networks. Breitinger et al. highlight a low level of adoption for protective VPNs [12], while [28] highlights that people are willing to use online banking on these networks. Given the use of HTTPS for most websites in the current day, security risks are likely minimal, however, other research highlights that public hotspot providers harvest and share significant amounts of personal data, based on tracking policies and information received through sign-ups or social logins [2].

Finally, some of the oldest security threats can develop new facets in the smartphone era, such as phishing, which users now also face in the forms of 'smishing' or 'vishing' (SMS/text and voice phishing via phone call, respectively). Importantly, as smartphones also overtake PCs for email usage [23] (although this is now harder to measure since Apple introduced features which made it impossible to track the device an email was opened on), users must adapt to identifying phishing emails on smartphones, but some research has identified that mobile email clients can hinder participants' ability to identify phishing emails by making important cues inaccessible [18].

Smartphones and their users face a broad number of threats, and attacks can be highly damaging and disruptive to users. The above research shows that as society continues to prioritize smartphones over PC platforms, threats and the required protective behaviors also develop, however, users do not always carry over applicable good habits between platforms, such as the use of security software (e.g., antimalware, VPNs) or application of skills and knowledge which have become obsolete (e.g., anti-phishing strategy). Updating our understanding of users' threat awareness and perceptions, and closely accounting for the use context of smartphones will allow us to develop training, interventions and design for more usable security in the smartphone era.

3 Method

This study used semi-structured interviews with smartphone users, covering topics relating to smartphone use, perceptions of the device's role in the users' life, and issues of security and protection of the device. Data was collected over the summer of 2021 and therefore a remote method was required to facilitate Covid-19 restrictions. Since telephone interviews may have the propensity to produce short answers [6] and recent research has found little difference in terms of topics discussed during exploratory interviews [30] the decision was made to use video interviews if possible, with audio-only interviews as a fallback. One-to-one interviews were selected to allow participants to openly express potentially private aspects of their smartphone use and types of data they keep. An inductive thematic analysis was used to explore the data, following the 6 step process outlined by Braun and Clark [11].

3.1 Participants

31 participants residing in the United Kingdom (mean age: 29.1 years, 14 Male, 13 Female) were recruited to take part in the study – however, due to a technical issue, the interview recording for participants 2-5 was unusable, thus they were excluded from the analysis, leaving us with a final sample of 27 participants. Our sample consisted of 16 iOS users and 11 Android users. Our sample and their occupations are summarised in Table 1 below.

Table 1: Summary of participant demographics

Participant	Age	Gender	OS	Occupation
1	27	M	IOS	Warehouse Worker
6	23	F	IOS	Student/Youth Support worker
7	24	M	Android	Customer Support
8	25	M	Android	Writer
9	23	F	IOS	Student
10	39	F	IOS	-
11	29	F	IOS	University Admin
12	33	F	Android	Carer
13	25	M	Android	Student
14	35	F	Android	Teacher
15	44	F	IOS	Teacher
16	34	F	IOS	Nurse
17	50	M	IOS	Sales Director
18	25	M	IOS	Train Station Staff
19	24	M	Android	-
20	26	F	IOS	Teacher
21	26	M	Android	Gardener
22	20	M	Android	Student
23	23	M	IOS	Teacher
24	25	F	IOS	Unemployed
25	35	M	IOS	Postgrad student
26	30	M	IOS	Lecturer
27	23	F	IOS	Doctor
28	29	F	IOS	Civil Servant
29	33	F	Android	Fitness Instructor
30	24	M	Android	Factory worker
31	32	M	Android	IT Technician

Participants were recruited via advertisements on social media platforms including Facebook, Twitter and Reddit and renumerated with an Amazon shopping voucher worth £15, except for one participant who declined to accept the payment. The study was approved by the department of [anonymised for review] ethics committee.

The inclusion criteria for participants were purposefully broad – they were required to be aged 18 years or over and a smartphone user. No specifications were set on the level or type of smartphone usage, allowing us to sample a wide range of smartphone users. While the smartphone operating system was not strictly an inclusion criterion, one prospective participant was excluded due to being a Windows Phone user. This decision was made due to Windows Phone no longer being supported; thus, the availability of up-to-date apps as well as issues of security and privacy would be somewhat different to those on supported operating systems (OS) such as Android and iOS.

3.2 Procedure

Participants were recruited to participate in a remote interview with the lead author. Participants were given the choice of communication platform for the interview. Interviews took place over Zoom (n=19), Discord (n=4), phone call (n=2), Microsoft Teams (n=1), and Jitsy.io (n=1). Participants were informed they would be taking part in an interview about the way they use their smartphone, how they view its role in their life and how they protect the device. Once informed consent was obtained, each interview was audio recorded and transcribed by the first author. The transcriptions were anonymized and any potentially identifying information was removed.

3.3 Interview Schedule

The semi-structured interview schedule was designed to cover several key areas of interest surrounding smartphone use and the user's perception of it. This allowed participants to further expand their experiences as smartphone users and elaborate on those areas they felt were most pertinent. The interview was arranged into 6 topics that began by establishing how participants used their smartphones, which would act as providing context for how and where participants may need to consider security alongside their usage. A more detailed interview schedule is available in appendix 1.

- Icebreaker style questions, collecting demographics and usage characteristics.
- Typical tasks and activities conducted on the smartphone, and the extent to which they relied on it in relation to other devices.
- The type of data kept on their phone, how they viewed the sensitivity and privacy of this data, and whether they protected or backed up the data.
- How they overall viewed the phone's role in their life.
- How participants protected their device and 'kept it secure' – this was open to interpretation as digital or physical security, allowing participants to express their immediate perception of maintaining their smartphone's security.
- The device's meaning and importance to them, and to judge if they felt the device was secure enough in light of how they use and perceive it.

After the study, we debriefed participants on our aims. As discussing security issues with participants may raise concerns (especially where many participants had given little thought to smartphone security before the interview), we offered participants the chance to ask any questions about threats, and how they could improve their personal security. We provided answers and reassurance for participants, and recommended websites where participants could learn more for themselves.

3.4 Analysis

Data analysis was conducted in NVivo 12, with the first author leading the process. The analysis process began with familiarization, followed by the generation of codes. Most codes identified were aligned with the issues we expected to discuss (e.g., specific dimensions of security and privacy or specific use contexts of the smartphone, such as for work purposes, day-to-day utilities etc.), however, some unexpected codes emerged such as discussion of how the Covid-19 Pandemic influenced smartphone usage and privacy. After coding data for all transcripts, the first author revisited each transcript to search for additional coding points which may have been missed earlier in the process, and to ensure the classification was consistent across transcripts. The codes were examined independently by the third and fourth authors who were each given 4 random transcripts to code. We found substantial overlap between our independent interpretations of the data and how it was coded. Following coding, themes were identified from observations made across multiple codes, producing two themes which were named by the authors. These are discussed in the results section below.

4 Results

4.1 Physical security first – mitigating unauthorised access

Summary: Participants expressed that their core security concern is around controlling physical access to the device. This was due to several factors: in a small number of cases, the uncertainty of the efficacy of their phone's locking mechanisms. For others, the financial value of the device itself meant it needed to be highly protected from loss or theft. For others, the smartphone is so critical to their everyday functioning that they maintain a high level of vigilance in ensuring they are never separated from it.

The physical nature of device security was foremost for the majority of participants as we posed open questions about how they protected their smartphone. Many participants considered how they physically looked after the device, namely protecting it from physical damage, by using cases and screen-protectors and remaining vigilant to prevent loss. Participants also focused on the physical aspect of the device when considering how they protect the integrity of their device from other people, with concerns around theft being voiced before that of 'hackers' or other digital bad actors. A small number of

participants suggested that the contents of their device could be easily accessed if a potential attacker had physical access to the device:

> "I have it password protected. But I believe people can get around that fairly easily. So, it's about physically protecting it." (P18).

> "I assume it is doable because hackers are amazing. And I guess it's just a passcode, it's not that intense is it really?" (P16).

Here, participants expressed a low level of confidence in their phone's locking mechanisms (particularly PIN/password locks), alongside high expectations of the abilities of attackers to be able to bypass locks. While this sentiment was voiced in the context of unknown attackers, a small number of participants considered that this threat was greater when considering those they knew closely, especially co-residing individuals, who had more opportunities to observe them enter a PIN/pattern and gain surreptitious physical access to the device. P21 considered that it would be very easy for people he lived with to access his phone and cause tangible damages, and relied on trusting that person to behave morally:

> "Like if somebody is going to get into your phone, well they're **going** to get into your phone, and most likely, it's going to be somebody you know closely, because they can just unlock it…I guess it's sort of a moral question but, if somebody is going to f**k me over like that… if you really want to take a look at my bank account and take a bunch of money out of it, go right ahead, but you're not gonna be able to sleep at night." (P21).

Similarly, P12 was confident in his phone's locking mechanisms ability to keep strangers out – but felt people who know him could succeed, as personal knowledge of pins or patterns is how unauthorized access occurs.

> "They couldn't get into my phone's data, they couldn't delete it …people wouldn't be able to get into my phone unless they knew me." (P12).

P12 alludes to their phone's unlock code being based on personal information; something which is common practice, as users often use dates such as birthdays and anniversaries for their PIN codes [10, 13, 38]. As P21 and P12 both suggest only people they know could get into their phone, it appears that users' approach to choosing a lock code may not be based on keeping out people they know, and instead trusting people close to them not to commit unauthorised access. However, research on unauthorised access has found that many people have previously 'snooped' through someone else's phone [34]. Research on unauthorised access does usually describe instances of a person known to the victim accessing the phone [33], however, this is usually intimate partners or close friends, with a social motive, not housemates as P21 described, nor for the purpose of financial gain. There may be a niche, yet prevalent angle to further explore, in which individuals who cohabit with individuals who are not close family, friends or partners may face damaging unauthorised access attacks that are enabled by shoulder surfing opportunities afforded by their living situation.

In more recent years, biometric locking has become standard across most new smartphones – offering new authentication approaches that are less easily defeated by shoulder surfing or prior knowledge of the individual. While early findings on biometrics' usability may be heavily influenced by the infancy of the technology [31], we can supplement these findings by exploring how users perceive the efficacy of biometrics further into their availability, as well as identifying the specific use contexts they find value in them for.

Biometrics, specifically fingerprint scanning largely seemed to be perceived as the most secure authentication method by participants, due to a lack of obvious means of being defeated unlike non-biometrics or face recognition:

> "It's a bit harder to game the fingerprint sensor, I think. You'd literally need my fingers. With more rudimentary face stuff or like a password, you could guess it, or you could like, fool it with a photo?" (P25)

Participants valued biometrics somewhat, as they offered an unintrusive way of adding extra security to sensitive apps, like a banking app, even if the phone itself could be unlocked by the less secure pattern/PIN unlock methods that are available as a backup for biometrics.

> "I find it quite creepy that my phone knows my fingerprint. Although, that's probably better than the tiny swiping pattern. I think if it wasn't for the fingerprint recognition thing, I'd [not] have my bank stuff on it." (P11)

On the other hand, to some participants, methods such as a fingerprint scanner were still seen as a 'gimmick', and by extension, less secure. P6 described an unusual instance where she was able to use her fingerprint to unlock her sister's phone, leading her to doubt the integrity of it as a locking mechanism:

> "One thing I have discovered with the thumbprint, though, is my sister has the same model of phone as me and when I put my thumb upside down on her phone it unlocks her phone…which makes me think that the thumbprint might be more of a gimmick than actually effective." (P6)

This observation does reflect theoretical findings that smartphone fingerprint scanners can be bypassed in a 'brute force' fashion using a 'master print', which is a synthetically generated fingerprint designed to mimic common characteristics of fingerprints, that could cause an optical fingerprint scanner to produce a false accept [46]. While such observations may have implications for perceptions of how secure a fingerprint scanner is, this interaction also builds upon the notion that co-residing people are most likely to commit unauthorised access, given that the fingerprints of

relatives may logically be seen as more similar, and thus more likely to unlock one's smartphone, which has some support in research indicating an influence of genetics on fingerprint formation [27, 48].

4.1.1 Motivations for physically protective behaviours.

We observed a number of factors that related to what motivated participants to prioritise the physical protection of their smartphone. While there were some doubts about the efficacy of locking mechanisms, the majority of participants were largely unconcerned about unauthorised access leading to actual harmful access to the phone. Even so, many participants reported that they felt the most important thing they had to do to protect the integrity of their smartphone was to remain attentive to the device physically, especially in public places. At face value, this aligns with older findings – that users prioritise physical vigilance of their phone [15], however, the motivation for doing so has changed. Participants of [15] feared their phones being lost or stolen, as it would mean they would lose the data stored on it. In the current day, this is far less of a concern, as the majority of our sample described their data being regularly backed up by automatic cloud syncing. Now, users appear motivated by two factors; first, the increasing cost of smartphones, and second, the immense reliance users have on their smartphones for everyday functioning.

When discussing how participants kept their smartphones safe, the high value of the device was a salient factor for a small number of participants, with theft being a prominent threat.

> "I am careful where I use it. So, while I was in [area], it's very clearly not the wealthiest part of town, and it was evening, so I didn't just whip out my smartphone and play games on the train like I might do [elsewhere]... because I've got an £800 computer in my hand, I'm conscious of that." (P25)

Smartphone pricing strategies have evolved over the past decade– while the average price has remained largely similar (including adjustment for inflation) [50], the disparity between premium and budget models has grown exceptionally, with budget models starting to plateau at low prices of below $100, whilst premium, flagship models continually break records for the 'most expensive smartphone to date'. Currently, the most premium smartphone models are around double their premium counterparts from 2012 (adjusted for inflation) [1]. This increase in value means that users now have to take much greater care of their smartphones as an expensive object.

While the high value of modern smartphones influences how a small number of participants used and protected their smartphones, this attitude could be entirely offset by insurance policies, where another subset of participants took a blasé attitude toward their phone if they were confident it would be replaced by an insurer.

> "It was very expensive, it's like 600 quid. So, that's why I have it insured you know, so I can get another one. If it breaks - whatever." (P21)

> "Like, if one of my kids threw it off the top of the stairs tomorrow, and it smashed, I know I can get a new device, I've got insurance. Yeah, new device, and then I upload everything I have to that from the clouds, I've got safety nets in place for it. (P29)

Interestingly, none of our participants stated the opposite; that they did not care for their smartphone because it was an older or cheaper model, however, it may still be a factor and could be an interesting avenue of future research, especially quantitative studies that can observe correlation between the smartphone's worth and the users' engagement with protecting the device.

Alternatively, some concerns about the device, and protecting it from loss or theft were not centered around the data on it, nor the cost of the device itself, but on how much users now rely on their smartphones for a vast range of everyday functions. The functional value of smartphones was almost unanimously agreed upon by participants, and a prominent concern for some who discussed the stress of being without it:

> "I feel like everything would be quite inconvenient, and it would feel a bit like losing an arm, because you're just so used to it being there all the time. I think I would find it a bit stressful...I feel like it just facilitates so much day to day like that." (P16)

The prospect of the phone being lost or stolen was clearly still a concern, even when there was no material loss at hand, and one participant offered their experience of losing their smartphone, detailing their emotions and the nature of their concerns.

> "Oh, it's a meltdown. About four weeks ago, I left it in a trolley in [a supermarket] ... And that moment, that hour of absolute, abject panic - not about what I've lost, but what I'm missing in terms of, who's rang me? What have I missed? And so, you know, I think the phone itself, you know, there's nothing contentious, nothing on it to be ashamed of, but it's more the fact that everything comes through that, it's the one conduit that makes my life tick." (P17)

Interestingly, amidst the panic caused by this situation, issues of security or privacy did not appear to weigh on P17's mind. For them, the loss of their 'conduit' was the primary concern, and the loss of connection to their digitally driven life was clearly an acute stressor. This need to maintain the hyperconnectivity offered by smartphones may act as a security motivator if users are highly cognizant of their smartphone's whereabouts and less likely to leave it behind or let it out of their possession. However, it also highlights that lost or stolen smartphones may cause great amounts of panic and stress, which may inhibit the user's ability to deal with the issue – such as retracing their steps to find it when lost, or using remote access features (e.g., Apple's Find My) to reclaim or secure the device if stolen. The high functional value of the smartphone may also offset lax attitudes to physical security caused by the presence of insurance on the device, as even with good insurance, users are likely to be without their device for several days until they receive a replacement.

While disregarding issues of security/privacy in this situation, another interesting factor in P17's response is around risks to the data on their smartphone. P17 had earlier acknowledged storing lots of sensitive work-related data, including private details of clients; the compromise of which could have vast consequences for himself, his employer, and the clients. This appeared to be part of a broader issue where participants didn't consider how sensitive data could be the target of security threats, instead focusing on more immediate damages, such as financial losses, which may occur through access to banking or other finance apps. Most participants did not store sensitive data on the same scale as P17, however there were still instances of sensitive information being improperly stored on the device, such as pictures of documents like passports, which participants often took for job applications and did not delete:

> "So [the smartphone] feels like it fulfils the same purpose as a scanner. So, here's a picture of my national insurance card if you need to see it, random employer" (P11)

Several participants also stored notes including passwords and other sensitive details; these notes were also not password protected. Only one participant seemed cognizant of the depth of unsecured data accessible through their smartphone, even where it wasn't directly stored on the device, but could be accessed via email apps:

> "If you can access my email, you can see stuff I've been sending to a mortgage advisor, which is like my [tax] forms, my husband's paychecks, our bank statements, things like that" (P29)

Participants concerns around data tended to be more related to sentimental data, pictures and videos of friends and families at memorable events. The idea of losing these was stressful to participants:

> "If I lost my phone, I would be absolutely gutted. Because there's years' worth of photos on it" (P22)

Many participants referenced using automatic cloud storage in place of manual backups, however there were signs that participants had a poor understanding of the cloud, or if their data was properly synced to it.

> "There are things on the cloud, but I find it confusing what the cloud is, although I do use it, but I don't really understand it." (P15)
>
> "Well, I think I've run out of storage. I don't know I keep saying I get notifications saying I've run out of storage. And to be honest, I feel like it's just a bit of a hassle." (P22)

This misconception around how cloud storage works is not a new finding [17, 43], however we highlight how smartphones contribute to poor personal and professional data management, which may have serious consequences, such as identity theft and other forms of fraud. It's clear that smartphones need to offer more transparent and usable cloud features, where users can understand if and how their data is backed up. Storage of sensitive documents could also be detected by algorithms that recognize if pictures of these documents (e.g. passports, other forms of ID) are stored on the device, and prompt the user to delete, or more securely store these files (e.g. in encrypted, password protected folders).

4.2 Digital security: Delegated at every turn

Summary: When discussing security threats of a digital nature, participants appeared to have little awareness or concern about threats of this nature. Participants expressed a high level of confidence in the phone and its software to be safe from security compromises, largely stemming from faith in well-known manufacturers and developers. When downloading content which may be considered risky, such as pirated media, participants identify other users as a source of validation for the legitimacy of websites and content. Participants express relying on reviews to assess the legitimacy of online content on their smartphones, despite an awareness these can be unreliable.

As discussed above, most participants interpreted our open question about securing the phone to be in relation to physical security. Following that stream of discussion, we would then prompt them to consider digital threats that may affect their phone. Initially, the idea that smartphones could be vulnerable to threats like malware was novel to two participants:

> "I think it's more of a threat to a laptop or something like that. Because I've not heard of anyone having viruses on their phone" (P14).

While most participants were conceptually aware of mobile malware, they still perceived the risk of this to be very low. This belief was largely centred around a high degree of trust in the apps they downloaded – partially coming from trust in the developer, but also from the use of centralised app stores which signalled to users that all the apps available to them are vetted by a major provider – either Apple or Google.

> "I just use the App Store, I think there's an element of security there because, to be able to get on there, they've got to prove to some extent that they're not just like a virus" (P1)

This demonstrates a change in the user's sense of responsibility in evaluating the validity of individual apps, where classically, computer users would only be able to download a program from its own specific website. This decentralized approach meant that users needed to personally take measures to evaluate several factors to safely download a program (i) that they have navigated to the correct website and not a malicious 'impostor' website, (ii) that they are downloading the intended content, as malicious advertisers would often create fake 'download button' styled ads to trick users into following a link to a different download to the one they intended [19] , and (iii) verifying if the downloaded software is conducting any illegitimate process, namely by using antimalware software. Now, smartphone app repositories centralize the process of downloading apps, and remove much of the ambiguity around individual downloads, visually assuring users with markers of legitimacy such as Android's 'Verified by Play Protect' message which displays when downloading applications from the Google Play store. This leads to a conscious difference between smartphone and PC platforms, where the user has a reduced sense of responsibility over security decisions.

> "But I suppose fresh out the box, I trust the phone more. Because with a laptop, you get an antivirus software. Whereas with the phone you don't necessarily do that. I mean, I imagine they probably exist, but I've never felt the need to do it." (P19)

In the same way that apps were seen as free from threats, participants viewed the smartphone itself as innately secure, and impervious to malicious software. This belief was generally credited to the reputation of the manufacturer, enough to prompt several participants to cite their smartphone's manufacturer as part of their overall security perception.

> "My phone's, a Samsung. So you do sort of tend to trust in the brand, don't you? They're a major tech company, they're going to know what they're doing in terms of their software." (P19).

This sentiment was particularly strong amongst the Apple (iPhone) users within the sample, who carried over a common idea that Apple computers were invulnerable to malware [49], to their smartphones:

> "I think it's more that Apple computers, everyone goes on about how they don't get viruses - that you can't get viruses for them. I think I actually kind of apply that sort of logic to my phone, 'cos my phone's made by the same people. So if Apple computers can't get viruses, I guess Apple phones probably can't?" (P1)

This is an interesting development from previous findings from 2012 [9], in which software developers are seen as most responsible for the security of smartphones by participants, with manufacturers and the user deemed to be least responsible. It now appears that users perceive manufacturers and developers to be jointly responsible for the entire smartphone ecosystem, rather than one individual sector being responsible.

These perceptions are largely reasonable; the app stores do validate apps, and manufacturers dedicate resources to maintain the integrity of devices. However, there are aspects of security and privacy that users still must take personal responsibility for, such as approving requested app permissions to access data or functionality of the smartphone.

> "No and to be honest, I'm really bad. Like, I never read them or anything, I just click okay….I think like I've used to feel a bit wary about having location services. But to be honest, it doesn't bother me anymore." (P20)

P20 demonstrates a lax attitude towards permissions which was the norm for the vast majority of our sample. However, a small number some were more aware and diligent over permissions, yet still fear they may inadvertently provide more access than they would like when habitually progressing through the installation process of a new app.

> "Well, when you download a new app, and it's like, this app wants access to your microphone, your saved information, your camera. And you're like, 'why? why do you want all this?' So, I don't know, it's not that I worry that I'm gonna download something, it's that I'm going to absentmindedly hit accept on an app that asks for access to my camera.' And then before you know it, I just gave someone access to my camera, with less than good intentions." (P30)

Most of our participants have a similar lack of attention to other security and privacy features that demand their approval, such as cookies and terms of service agreements:

> "There's probably terms and conditions that you kind of sign up for whenever you download anything. Do you read them? Probably not… it's a sort of consciousness of not knowing, assuming that everything is probably fine." (P11)

> "Initially, I used to read each and every cookie before accepting it. But, for each and every page it asks me to accept cookies and when I'm in a situation where I can't [read them], I just accept it and move forward. I think nobody likes to do that, but sometimes you have no other choice in accepting it" (P13)

These agreements are too frequent, and/or too demanding for users to consistently process and manage the data they give away. In addition to privacy agreements, we observed that changes stemming from Covid-19 restrictions introduced further privacy concerns that participants felt powerless to manage. As individuals were allowed to return to hospitality venues post-lockdowns, bars and restaurants facilitated social distancing through smartphone apps to view menus and order. One participants described these as another source of diminished privacy through their smartphone:

> "Previously I would go to a pub, and I would order two drinks, and I would pay for them with a card … and now it's like, oh, here's an app, or I'm just gonna give them all my card details, and my address, and my name, and my shoe size. Because that's the only way I can get a pint." (P11)

Clearly, these systems encourage users to disclose more personal details than they would like, but resisting the collection of their data is too troublesome, or otherwise interferes with normal life, benefitting entities that collect and monetize this data. Ignoring and/or clicking through privacy and permission notices is clearly becoming a habit, furthering observations from previous literature (not focused on mobile devices) which identified that users tend to ignore security notices/warning [4]. The same systems of security notices are prevalent across operating systems, but seemingly appear more frequently and in situations where users can seldom afford the proper attention to deal with them as they would like, creating a habit of disregarding all notices that can be clicked through.

The issue of habituation is often recognized, but poorly understood in security research as broader theory around changing habit formations and habitual behaviors are not utilized in security and privacy contexts [59]. Future research and legislation around privacy notices (e.g., cookie requests) must endeavor to find useable ways for users to manage their privacy that do not overload users and lead to habitual click-through behaviors.

4.2.1 Uncharted waters: how mobile pirates make security judgements.

We discovered one dimension of digital security in which participants are aware of a greater level of risk which should require more vigilance. This was in relation to downloading illegitimate content to their smartphones such as pirated media including music, video, and eBooks. Pirated content is associated with security risks, as malicious websites often use free downloads of media as a pretence for delivering malware to unsuspecting users. The two participants who engaged with pirated content on their smartphones recognized this risk, yet seemed unaware of how they could reliably verify the safety of any downloads. Users reported relying on their fellow users to identify the safety of apps or online content, through user reviews left on the websites – believing that if a download was suspicious or illegitimate, there would be reviews from other users warning about this.

> "It's not that I trust the providers of the downloads, but the community. I think people would comment and if, for instance, there was a comment "Oh, this thing had a virus" or whatever, no one would download it. And then eventually, the torrent would just fade away because no one's downloading it." (P8)

This is a highly unreliable method of determining the safety of online content, given the potential for reviews which are faked by owners of an illegitimate website, and for fake/bot accounts to appear legitimate. Surprisingly, participants did acknowledge the unreliability of this method, yet still relied on it, as they felt they had no better or safer method available to them.

> "I know as simple as it might seem, you know, I look at reviews. And obviously reviews can be bought, that's a thing, but I like to look at reviews" (P30).

When it comes to downloading content, which may compromise their device, participants seem to lack an objective method of evaluating the authenticity of the sources outside of the app stores, or how to assess the safety of downloaded files (e.g., scanning for malware/spyware). Both P8 and P30 were aware of how to use anti-malware on their computers and reported previously choosing, installing, and making use of scanning tools when downloading pirated content on a PC before smartphones became their primary platform, yet this behaviour appears to have not transferred to their smartphone. When prompted to consider why they do not try to use anti-malware features on their smartphone, the participants in question indicate that they simply did not view it as necessary on this device.

> "No, I think the risk is quite small. And like, there's a certain level of security that's baked into the software. So, I don't think it's worth it really, for me." (P8)

The assumption that the smartphone's software is innately secure connects back to our above findings, that the centralized nature of the smartphone ecosystem primes users to defer their responsibility for vigilance and validation of content they download, which poses a legitimate problem for users who do venture beyond their native app repository.

While relying on user reviews may seem to indicate a lower level of technical expertise, more expert participants in the sample expressed similar levels of community trust, albeit outside of the pirate context. P31, a senior IT specialist, expressed a preference for using open-source apps, where the transparent nature of the software allows users to see how the software operates and if any illegitimate functions are present. However, P31 did not personally verify the legitimacy of such software, instead assuming other 'smarter' users would do so.

> "I'm quite lazy, I don't always check. But the ability to do that is quite nice, because there's a lot more smarter people looking at it and going 'yeah, that's perfectly fine'" (P31).

In instances like this, participants are hoping that simply by virtue of being open source, it is unlikely an app would attempt illicit actions, because 'someone' would uncover this.

In this theme, we observed how participants expressed trust in their devices and the apps they use to be naturally immune to security threats. In cases where they acknowledge a human judgement is needed to identify risks associated with a download, participants are inclined to rely on the hive mind of internet communities to alert them to dangerous content. Additionally, these findings develop upon those of previous research which show smartphone users commonly fail to engage in behaviours such as installing and using antivirus software on their phones, even when they would do so on their computers [3, 12, 51]. Despite acknowledging their smartphones as 'little computers', participants fail to treat them as computers, at least from a security perspective, expressing a level of faith in manufacturers and developers to negate threats.

5 Discussion

We analysed 27 interviews with participants about the significance of their smartphones in their lives, and the relationship this has with their perceptions of security and adoption of security behaviours. We find that security perceptions in the 2020s have changed considerably in the last ten years. Our core findings are as follows: First, smartphones are more valuable than ever, both monetarily, and in terms of their functional importance – leading users to place great emphasis on physically protecting their device, even if its content is backed up and data loss is unlikely. Second, users are now well accustomed to the centralized nature of smartphone ecosystems, where the apps available to them are assumed to be carefully vetted by app stores – perhaps creating a false perception that apps will not act harmfully and either abuse data collection or permissions. This sense of security seems to be reflected in high levels of trust in recognized manufacturers (e.g. Samsung, Apple). Thirdly, frequent, unusable privacy notices and requests within a trusted app store lead to users becoming habituated to ignoring or disregarding such requests, even outside of the relative

safety of the app store. This habituated acceptance of requests means that third parties can gain excessive control over their device and data. Finally, a small number of individuals engage in piracy on their smartphone – a behaviour they know is risky and use protective measures when downloading pirated media onto a PC, but fail to transfer these behaviours over to the smartphone platform, perhaps making this the most plausible way smartphone users could be vulnerable to malware. We discuss further implications of these findings below.

5.1 Security perspectives in the 2020's – a decade of building brand trust

An important point of comparison for our study is Chin et al.'s study from 2012 [15]. They explored user perceptions of privacy and security on their smartphones in relation to a broad set of behaviours, with specific comparisons made to the same behaviours being carried out on computers. We observe that behaviours which participants of [15] avoided due to mistrust in the security of their devices and app developers are now commonplace. Our participants, now seasoned smartphone users, show this mistrust in service providers is no longer prevalent; behaviours like mobile banking and online shopping are a core function of the smartphone within our sample, as well as society at large [24, 37]. There may be two reasons for this – the normalization of these behaviours across society is likely to give users faith in the safety of carrying out sensitive tasks on their smartphones. Yet a major factor we observed is that long-established smartphone manufacturers appear to have earned a level of trust that was not present in 2012, with participants expecting innately secure products, demonstrating strong 'brand trust'.

Brand trust is described as "consumers' confidence in the quality and trustworthiness of the products provided" [22]. Typically, this sense of trust is viewed as contributing to perceptions of consistency one can expect from a company's goods or services, and is not typically measured against factors such as cybersecurity. Some findings do indicate that brand trust extends to the cybersecurity perceptions of smartphones – however, this has primarily been observed in relation to app developers [9], and app repositories (e.g. Google Play, Apple's App Store) [40]. We find that manufacturers and their brand reputation also influence user security perceptions.

The influence of brand trust has been observed in previous findings; it has classically applied to Apple computers, with a common conception that Apple Macs are invulnerable to security exploits, previously referred to as 'The Mac Factor' [49]. Our findings suggest not only that the Mac Factor extends to iPhones (and thus may be more broadly titled as 'The Apple Factor'), but that similar effects apply to other major brands such as Samsung, albeit to a seemingly lesser extent than the Apple Factor affords. This brand trust likely has interplay with the impact of the smartphone's monetary value, as some participants discussed greater protectionism over their smartphone in the context of its cost; these higher price tags are synonymous with the more premium brands, Apple and Samsung. However, with Apple and Samsung making up less than half of the smartphone market share globally [47], smaller and less premium brands such as Oppo and Xiamoi also hold a significant market share. While our participants did use a variety of smartphones from different manufacturers, no participants cited their smartphone's manufacturer in relation to security outside of Apple and Samsung users, so the role of the manufacturer, and its brand perceptions remain unclear. Further quantitative work on the relationship between brands and security work is required. Researchers may consider quantifying security engagement (using measures such as [56]) and make comparisons between manufacturers, or other factors related to the value of the phone, including its age, model, insurance status and monetary value as a device that provides connection to many other functions such as email, finance, home security, etc. An important question to explore is whether the financial cost of phone ownership has resulted in behaviour that indirectly protects online assets through the physical protection of the device, and if this protectionism could be lost where the phone is cheaper or older.

5.2 (Mis)handling security responsibility

While users delegate a great amount of security responsibility to developers and manufacturers, there are two key areas they acknowledge having responsibility for: (i) Managing apps permissions and user agreements (cookies, terms of service) and (ii) protecting their device from physical threats such as loss or theft.

When it comes to managing permissions and user agreements, participants clearly expressed both security and privacy fatigue towards handling these frequent requests for approvals. Previous research has identified that smartphone users experience privacy fatigue, specifically in relation to frequent and often complex user agreements [16, 52]. We add to this field of knowledge by considering that the threat perception around approving permissions/user agreements may be mediated by the level of trust stemming from the centralized nature of the smartphone ecosystem, compromising the extent to which they truly take responsibility for handling these agreements. Participants believe their apps and software are vetted and secured by reputable providers (i.e., the native app stores) – so when presented with the need to approve or agree to something, they are conditioned to believe that whichever option they take will be safe and appropriate.

The faith in their smartphone's closely protected ecosystem remained even in edge cases where participants downloaded from outside of an app store or went 'off grid' and downloaded pirated media. Two of our Android-using participants described seeking out free eBooks, music, and other media, which they acknowledged could contain malware. Despite the experienced pirates in our sample claiming to understand the importance of using an antivirus program on their PC while downloading pirated content, this behaviour did not carry over to their smartphones, providing a critical point of vulnerability for these participants. This is indicative of good security behaviours failing to transfer to smartphone platforms, now that the behaviour when users have become familiar with the platform, over an extended

period where anti-malware was not as necessary. On Android platforms, where users have greater freedom to download third party apps and other content, it appears that the operating system could more clearly emphasise that downloaded content may be harmful, and to encourage use of anti-malware.

Physical security was a dimension in which users recognised their responsibility, and actively engaged in protective behaviours and vigilance. Where physical security was previously established as a priority of users [15], we update the context of this priority, demonstrating it is no longer a means of preserving data stored on the smartphone, but due to both the sharply rising price of premium smartphones, and the high level of stress associated with being separated from their smartphone due to their reliance on its functionality, and the need for constant connectivity for work and social purposes. While the latter motive may act as a useful security motivator for participants, the acute stress incurred from losing the device may be counterproductive in hindering the user's ability to use remote access features to find or secure the phone. While all modern smartphones can enrol on 'find my phone' features, it seems users require more explicit support in understanding how they can use these to locate their device, and the features available to support them in managing risks associated with the phone being lost (e.g. data back-ups, more stringent locking). This information should be presented to users upon setup of a new device, or by prompting users who have not setup such services to consider exploring the available features at certain intervals, e.g. every 6 months.

The cost of smartphones may be an interesting factor to explore; as participants with high-value devices cite this as a motive to protect it more, however, the monetary value of the smartphone is likely to be relative to the owner and their finances. A low-cost device may still be difficult to replace, and users of lower socioeconomic status are also more likely to be 'smartphone dependent' [57], in that their smartphone is their only means of accessing the internet. Therefore, whilst the cost of the device likely does play a role in many users' security motives, it is also likely to be part of a more complex interplay of factors, including their ability to buy another device if needed, if insurance could offset this, and how functionally reliant they are on the device that would necessitate the urgency of replacing their device if lost or stolen.

5.3 Limitations and future work

We introduce several new factors that can be explored in future work relating to smartphone security behaviors and perceptions. Some of the key questions further research should answer include:

- How do financial factors influence security perception/behavior, including the monetary value of the phone, socioeconomic status of the user, and insurance status of the phone?
- How the brand/manufacturer identity influences security perceptions of the device – are there differences between premium manufacturers like Samsung and Apple, versus less premium models such as Xiaomi or Oppo?
- How different bad actors may play different roles in unauthorised access – do cohabiting individuals such as roommates pose a unique threat, where they have elevated access to the device, but less of a close relationship to dissuade harmful attacks?
- How do users make decisions on trust and security when downloading media or apps from outside of established platforms such as an official app store? Why do users adopt different behaviours to the same behaviours on a PC?

Having identified these new factors, quantifying them is a logical next step that would allow us to support our hypotheses that these factors influence security perceptions and, consequently, behaviors. This may be accomplished using threat models such as Protection Motivation Theory, where the perceived severity related to threats against the smartphone may be affected by factors such as the cost of the phone, or its insurance status. Similarly, there may be differences in Threat Vulnerability perceptions between users of different phone brands.

Our study is not without limitations – some factors relating to our sample should be considered as possibly influencing our findings. In an effort to capture a broad and diverse set of smartphone users, we put no real limitations on the type of smartphone user we sampled. While this did let us sample participants who appeared to be more intensive users, as well as those who were more casual users, we cannot guarantee our sample are broadly representative of smartphone users. Another factor is that our sample's average age is relatively young – 29. While we did sample from local community-related groups on social media (and not institutions such as universities, which often produce younger samples), we had little representation from middle- or older-aged participants, whose perspectives may have enriched our dataset and conclusions. Further research could consider ensuring greater representation, or specifically focusing on older adults. Finally, social desirability bias may have influenced participants' answers to our questions. In the context of security, participants may wish to appear more careful knowledge or concerned with security threats when under the impression that the researcher feels they should be. Whilst we endeavoured to remain neutral in our interviews, social desirability is always a possible influence on participants.

6 Conclusion

We present qualitative findings on user perspectives of how they secure their smartphone, with a particular emphasis on the context of modern smartphone usage, and how a smartphone's role in everyday life affects their importance to

users, and by extension, how users protect the device. We identify several factors affecting users' perceptions and the actions they take (or don't take) to remain secure and propose how future research may explore these factors further. This work demonstrates the importance of refreshing existing findings in areas where technology has evolved rapidly, as user perceptions are also likely to have evolved. It is essential that research insights are kept up to date so that both researchers and developers who make use of such knowledge are not building on outdated foundations.

References

[1] Ali, R. 2020. Mobile phone prices soar over 20 years. *uSwitch*. (Jul. 2020). DOI:https://doi.org/https://www.uswitch.com/mobiles/news/2020/07/mobile-phone-prices-soar-over-20-years/.

[2] Ali, S., Osman, T., Mannan, M. and Youssef, A. 2019. On Privacy Risks of Public WiFi Captive Portals. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 11737 LNCS, (2019), 80–98. DOI:https://doi.org/10.1007/978-3-030-31500-9_6.

[3] Alsaleh, M., Alomar, N. and Alarifi, A. 2017. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE*. 12, 3 (Mar. 2017), e0173284. DOI:https://doi.org/10.1371/journal.pone.0173284.

[4] Amran, A., Zaaba, Z.F. and Mahinderjit Singh, M.K. 2018. Habituation effects in computer security warning. *https://doi.org/10.1080/19393555.2018.1505008*. 27, 4 (Jul. 2018), 192–204. DOI:https://doi.org/10.1080/19393555.2018.1505008.

[5] Android app breaking bad: From legitimate screen recording to file exfiltration within a year: 2023. *https://www.welivesecurity.com/2023/05/23/android-app-breaking-bad-legitimate-screen-recording-file-exfiltration/*. Accessed: 2023-06-02.

[6] Arksey, H. and Knight, P.T. 1999. *Interviewing for Social Scientists: An Introductory Resource with Examples*.

[7] Bandura, A. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*. 84, 2 (Mar. 1977), 191–215. DOI:https://doi.org/10.1037/0033-295X.84.2.191.

[8] Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A. and Möller, S. 2011. On the need for different security methods on mobile phones. *Mobile HCI 2011 - 13th International Conference on Human-Computer Interaction with Mobile Devices and Services* (2011), 465–473.

[9] Benenson, Z., Kroll-Peters, O. and Krupp, M. 2012. Attitudes to IT security when using a smartphone. *2012 Federated Conference on Computer Science and Information Systems, FedCSIS 2012* (2012), 1179–1183.

[10] Bonneau, J., Preibusch, S. and Anderson, R. 2012. A birthday present every eleven wallets? The security of customer-chosen banking PINs. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 7397 LNCS, (2012), 25–40. DOI:https://doi.org/10.1007/978-3-642-32946-3_3.

[11] Braun, V. and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*. 3, 2 (2006), 77–101. DOI:https://doi.org/10.1191/1478088706qp063oa.

[12] Breitinger, F., Tully-Doyle, R. and Hassenfeldt, C. 2020. A survey on smartphone user's security choices, awareness and education. *Computers and Security*. 88, (Jan. 2020), 101647. DOI:https://doi.org/10.1016/j.cose.2019.101647.

[13] Casimiro, M., Segel, J., Li, L., Wang, Y. and Cranor, L.F. 2020. A Quest for Inspiration : How Users Create and Reuse PINs. *WAY* (2020).

[14] Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D. and Ristenpart, T. 2018. The Spyware Used in Intimate Partner Violence. *Proceedings - IEEE Symposium on Security and Privacy*. 2018-May, (Jul. 2018), 441–458. DOI:https://doi.org/10.1109/SP.2018.00061.

[15] Chin, E., Felt, A.P., Sekar, V. and Wagner, D. 2012. Measuring user confidence in smartphone security and privacy. *SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security* (2012).

[16] Choi, H., Park, J. and Jung, Y. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*. 81, (Apr. 2018), 42–51. DOI:https://doi.org/10.1016/J.CHB.2017.12.001.

[17] Clarky, J.W., Snyder, P., Mccoyy, D. and Kanich, C. 2015. I saw images I didn't even know I had : Understanding user perceptions of cloud storage privacy. *Conference on Human Factors in Computing Systems - Proceedings*. 2015-April, (Apr. 2015), 1641–1644. DOI:https://doi.org/10.1145/2702123.2702535.

[18] Dixon, M., Nicholson, J., Branley-Bell, D., Briggs, P. and Coventry, L. 2022. Holding Your Hand on the Danger Button: Observing User Phish Detection Strategies Across Mobile and Desktop. *Proceedings of the ACM on Human-Computer Interaction*. 6, MHCI (Sep. 2022), 1–22. DOI:https://doi.org/10.1145/3546730.

[19] Duman, S., Onarlioglu, K., Ulusoy, A.O., Robertson, W. and Kirda, E. 2014. TrueClick: Automatically Distinguishing Trick Banners from Genuine Download Links. (2014). DOI:https://doi.org/10.1145/2664243.2664279.

[20] Egelman, S., Jain, S., Portnoff, R.S., Liao, K., Consolvo, S. and Wagner, D. 2014. Are you ready to lock? Understanding user motivations for smartphone locking behaviors. *Proceedings of the ACM Conference on Computer and Communications Security* (2014), 750–761.

[21] Frik, A., Kim, J., Rafael Sanchez, J. and Ma, J. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings; Users' Expectations About and Use of Smartphone Privacy and Security Settings. *CHI Conference on Human Factors in Computing Systems*. (2022). DOI:https://doi.org/10.1145/3491102.

[22] Garbarino, E. and Johnson, M.S. 1999. The Different Roles of Satisfaction, Trust, and Commitment in Customer Relationships. *Journal of Marketing*. 63, 2 (1999), 70–87. DOI:https://doi.org/10.1177/002224299906300205.

[23] Global email platform market share 2021: 2022. *https://www.statista.com/statistics/709596/most-used-e-mail-platform-by-market-share/*. Accessed: 2023-06-02.

[24] Great Britain: online banking use 2020: 2020. *https://www.statista.com/statistics/286273/internet-banking-penetration-in-great-britain/*. Accessed: 2022-05-09.

[25] Harbach, M., De Luca, A., Malkin, N. and Egelman, S. 2016. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. *Conference on Human Factors in Computing Systems - Proceedings* (2016), 4823–4827.

[26] Harbach, M., von Zezschwitz, E., Fichtner, A., Luca, A. De and Smith, M. 2016. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. *SOUPS '14: Proceedings of the Tenth Symposium On Usable Privacy and Security*. (2016), 213–230.

[27] Ho, Y.Y.W. et al. 2016. Genetic variant influence on whorls in fingerprint patterns. *The Journal of investigative dermatology*. 136, 4 (2016), 859. DOI:https://doi.org/10.1016/J.JID.2015.10.062.
[28] Imgraben, J., Engelbrecht, A. and Choo, K.K.R. 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *http://dx.doi.org/10.1080/0144929X.2014.934286*. 33, 12 (Dec. 2014), 1347–1360. DOI:https://doi.org/10.1080/0144929X.2014.934286.
[29] Jones, B.H. and Chin, A.G. 2015. On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management*. 35, 5 (2015), 561–571. DOI:https://doi.org/10.1016/j.ijinfomgt.2015.06.003.
[30] Krouwel, M., Jolly, K. and Greenfield, S. 2019. Comparing Skype (video calling) and in-person qualitative interview modes in a study of people with irritable bowel syndrome-an exploratory comparative analysis. *BMC Medical Research Methodology*. 19, 1 (Nov. 2019), 1–9. DOI:https://doi.org/10.1186/S12874-019-0867-9/TABLES/4.
[31] De Luca, A., Hang, A., Von Zezschwitz, E. and Hussmann, H. 2015. I feel like i'm taking selfies all day! towards understanding biometric authentication on smartphones. *Conference on Human Factors in Computing Systems - Proceedings* (2015), 1411–1414.
[32] Markelj, B. and Bernik, I. 2015. Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*. 20, (Feb. 2015), 84–89. DOI:https://doi.org/10.1016/j.jisa.2014.11.001.
[33] Marques, D., Guerreiro, T., Carriço, L., Beschastnikh, I. and Beznosov, K. 2019. Vulnerability & Blame: Making sense of unauthorized access to smartphones. *Conference on Human Factors in Computing Systems - Proceedings* (2019).
[34] Marques, D., Muslukhov, I., Guerreiro, T., Beznosov, K. and Carriço, L. 2019. Snooping on mobile phones: Prevalence and trends. *SOUPS 2016 - 12th Symposium on Usable Privacy and Security* (2019), 159–174.
[35] Mehrabi Koushki, M., Obada-Obieh, B., Huh, J.H. and Beznosov, K. 2020. Is implicit authentication on smartphones really popular? On android users' perception of "smart lock for android." *Conference Proceedings - 22nd International Conference on Human-Computer Interaction with Mobile Devices and Services: Expanding the Horizon of Mobile Interaction, MobileHCI 2020* (2020), 17.
[36] Miller, D., Abed Rabho, L., Awondo, P., de Vries, M., Duque, M., Garvey, P., Haapio-Kirk, L., Hawkins, C., Otaegui, A., Walton, S. and Wang, X. 2021. The Global Smartphone. *The Global Smartphone*. (May 2021). DOI:https://doi.org/10.14324/111.9781787359611.
[37] Mobile E-commerce is up and Poised for Further Growth: 2018. *https://www.statista.com/chart/13139/estimated-worldwide-mobile-e-commerce-sales/*. Accessed: 2022-05-09.
[38] Munyendo, C.W., Markert, P., Nisenoff, A., Grant, M., Korkes, E., Ur, B. and Aviv, A.J. 2022. "The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits. *Proceedings of the 31st USENIX Security Symposium, Security 2022* (2022), 4023–4040.
[39] Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J. and Beznosov, K. 2013. Know your enemy: The risk of unauthorized access in smartphones by insiders. *MobileHCI 2013 - Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services* (2013), 271–280.
[40] Mylonas, A., Kastania, A. and Gritzalis, D. 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers and Security*. 34, (2013), 47–66. DOI:https://doi.org/10.1016/j.cose.2012.11.004.
[41] Ofcom 2015. *The Communications Market Report (2015)*.
[42] Perrin, A. 2021. *Mobile Technology and Home Broadband 2021*.
[43] Ramokapane, K.M., Rashid, A. and Such, J.M. 2019. "I feel stupid I can't delete...": A study of users' cloud deletion practices and coping strategies. *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017* (2019), 241–256.
[44] Reinfelder, L., Benenson, Z. and Gassmann, F. 2014. Differences between Android and iPhone users in their security and privacy awareness. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2014), 156–167.
[45] Rogers, R. and Prentice-Dunn, S. 1997. Protection motivation theory. *Handbook of health behavior research 1: Personal and social determinants*. (1997), 113–132.
[46] Roy, A., Memon, N. and Ross, A. 2017. MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems. *IEEE Transactions on Information Forensics and Security*. 12, 9 (2017), 2013–2025. DOI:https://doi.org/10.1109/TIFS.2017.2691658.
[47] Sing Waila, H. 2022. *MOBILE DEVICES MONITOR – Q2 2022*.
[48] Slatis, H.M., Bat-miriam Katznelson, M. and Bonne-tamir, B. 1976. The Inheritance of Fingerprint Patterns. *Am J Hum Genet*. 28, (1976), 280–289.
[49] Stafford, T., Deitz, G. and Li, Y. 2018. The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*. 33, 4 (2018), 410–424. DOI:https://doi.org/10.1108/MAJ-07-2017-1596.
[50] Statista Consumer Market Insights 2022. *Global: average smartphone price 2013-2027*.
[51] Taha, N. and Dahabiyeh, L. 2021. College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*. 26, 2 (2021), 1721–1736. DOI:https://doi.org/10.1007/s10639-020-10330-0.
[52] Tang, J., Akram, U. and Shi, W. 2020. Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits. *Journal of Enterprise Information Management*. 34, 4 (2020), 1097–1120. DOI:https://doi.org/10.1108/JEIM-03-2020-0088.
[53] Taylor, B.Y.K. and Silver, L. 2019. *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*.
[54] The number of mobile malware attacks doubles in 2018, as cybercriminals sharpen their distribution strategies: 2019. *https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies*. Accessed: 2021-04-09.
[55] The Pegasus project: 2021. *https://www.theguardian.com/news/series/pegasus-project*. Accessed: 2023-06-02.
[56] Thompson, N., McGill, T.J. and Wang, X. 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers and Security*. 70, (Sep. 2017), 376–391. DOI:https://doi.org/10.1016/j.cose.2017.07.003.
[57] Tsetsi, E. and Rains, S.A. 2017. Smartphone Internet access and use: Extending the digital divide and usage gap. *Mobile Media and Communication*. 5, 3 (2017), 239–255. DOI:https://doi.org/10.1177/2050157917708329.
[58] Watson, B. and Zheng, J. 2017. On the User Awareness of Mobile Security Recommendations. *Proceedings of the SouthEast Conference*. 8, (2017). DOI:https://doi.org/10.1145/3077286.

[59] Weickert, T.D., Joinson, A. and Craggs, B. 2023. Is cybersecurity research missing a trick? Integrating insights from the psychology of habit into research and practice. *Computers and Security*. 128, (May 2023). DOI:https://doi.org/10.1016/J.COSE.2023.103130.

Appendices

Appendix 1 – Code list and frequencies

Code	Presence in # of transcripts	Total occurrences
Attitude to phone's role in life	25	120
Role of large companies	17	41
Phone's role in communication and socializing	24	71
Discussion of data types and storage behaviours	27	100
Pandemic influences	7	9
Permissions	18	30
Privacy issues	19	61
Safety features	12	27
Scams	8	10
Security issues	27	231
Work uses of smartphone	11	33

Appendix 2 – Interview questions. Note that not all sub questions were asked in every interview– these were prompts for where participants needed further encouragement/specificity.

Intro/icebreaker

- What kind of things do you use your smartphone for?
- What kind of smartphone do you have? (iphone, android, other)
- Do you have multiple smartphones? E.g. separate work phone
- How much would you say you use your smartphone for on a usual day?
- Is most of your smartphone use tied to recreational purposes (i.e. socialising, browsing social media, other recreational things i.e. Netflix, YouTube), are there many practical things you use it for, i.e. work?

Smartphone's role

- How frequently do you use your smartphone?
- Do you feel like you depend on your smartphone in any way?
- Do you think you could live without your smartphone?
- Are there ever times you don't have your smartphone around you? Do you leave home without it?
- Do you have a laptop or computer?
    - Do you use it much compared to your smartphone?
    - What tasks do you decide to use for certain devices?

Functions

- Is your smartphone important to your social life?
    - Conversations, planning social activities etc.
    - Would you lose touch with any people without your smartphone?
    - Would it be harder to keep in touch with friends/family without your smartphone?
- Is your smartphone important to your work/academic responsibilities?
    - Could you still do your job without your smartphone?
- How much do you need your smartphone for day-to-day tasks?
    - Using it as bank card/payment method
    - Public transport tickets / other events tickets
    - Contact tracing/ track and trace apps?

    - Placing orders for food/drink?
    - Anything else?
- Do people often need to be able to reach you via your smartphone?
    - Communicating with family, perhaps relating to childcare, care of older relatives
    - Just wanting to be reachable – FOMO, connectedness
- Is your smartphone essential to access certain accounts – i.e. use 2FA through it
    - Access to bank account (i.e. generating security codes)
    - Receiving other 2FA codes – general accounts, government accounts, work accounts
- Do you depend on your smartphone for your safety?
    - Specific apps, or simply texting/calling to confirm safety of self and others
    - Location sharing (Whatsapp, Facebook, various family trackers etc.), Personal Alarms (e.g. Onescream), journey monitoring (Kitestring, built in features to Uber etc.)
    - Find my phone/friends – who has access, ever needed before? Any misuse of it by friends?

Data

- What kind of data does your smartphone store?
- Any important or sentimental data?
    - Photos – family, friends, pets etc. – backed up or not?
    - Contacts – phone numbers, addresses
    - Important info – notes, reminders (saved on device, not a calendar through outlook etc.)
    - Copies of ID such as password, drivers license, other documents
- Does your smartphone store sensitive or secret information? (i.e. things you wouldn't want anyone to have) – Things that you might consider 'for your eyes only'
    - Notes of passwords
    - Bank details
    - Private conversations
    - Private files/intimate pictures, videos etc
- Do you do anything to keep this data secured?
    - Encryption, locked folders, cloud storage etc.

Feeling

- How would you feel if you lost your smartphone?
    - what would be your main concern/issue around this
        - – the monetary value of the device/replacing it or loss of data that was on the device, or access to certain functions, contacts etc., content you'd be embarrassed about (i.e. sexting etc.)?
- Would your smartphone becoming lost or damaged disrupt your life much?
    - Would it take much adjustment to get back to normal without it?
- How important is your smartphone to you?
    - In what ways?
    - As a tool? Medium for socialising, learning etc.
    - Any emotional connection – to the device or just it's functions/data?
- Have you thought about these things before this conversation?

Security behaviours

- How do you look after your phone and keep it secure?
    - Cover both sides – physical/cyber
- How much do you prioritise keeping your smartphone (secure)?
- How do you keep your smartphone safe?
- Do you have some kind of lock on your phone?
    - Do any other people know your lock code?
- Do you share your device with anyone?
    - Specifically a shared device, or just giving to friend/partner sometimes?
    - Supervised? What do they get to use it for?
- Do you often consider security while using your smartphone?
    - What tends to bring security to your mind when using your smartphone?
    - Have you ever had a security issue on your smartphone?
- What kind of security risks do you think are most likely to affect your smartphone?
- Do you consider your smartphone to be more at risk to security issues than your computer/laptop?
    - Do you use any kind of security software/apps on your phone? On your computer?

- Do you often notice when apps request permissions?
    - How much attention to do you pay to these?
    - How do you usually respond to these requests?
- Do you download apps that aren't on your device's app store?
    - Where from/what for/why?
    - Do you take any precautions around downloading/installing these apps?
- Do you have passwords for specific apps/accounts on your smartphone? (that don't stay logged in – banking app most likely will, for example)
- Are there important files or pieces of information saved on your smartphone, such as copies/pictures of ID, lists of passwords etc.
    - If so, are these files protected in any way? (password protected folder, encryption, Backed up?)
- Have you ever considered how you might respond to a security issue on your smartphone?
    - Do you think you'd be able to deal with it yourself?
    - What would you be most concerned about losing? Data? Access to certain apps/functions?
    - If you're unsure you'd be able to deal with it yourself, do you have an idea of where you could get help? (Techy friends, tech support info online, tech support from businesses?)
- Do you keep your software up to date?
    - Auto updates?
    - The smartphone's OS?
    - Specific apps?
- Have you ever disabled/removed a safety feature?
    - Which one? Why?
- Do you have some kind of locking mechanism on your phone?
    - Do any other people know your lock code?
- Do you feel your smartphone is secure enough without needing lots of attention?
- Do you feel the same about other devices, i.e. computer?

Security/value match

- Reflecting on your smartphone's role in your life, and how you secure it, do you feel you keep it secure enough?
    - Do you have enough specific protections in place, or act secure enough?
    - Is there anything you think is under-protected on/about your device?
    - Do you feel prepared for any security incidents that might happen to you
    - Anything you know you want to change now?