Better the Devil You Know: Using Lost-Smartphone Scenarios to Explore user Perceptions of Unauthorised Access

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

Smartphones are a central part of modern life and contain vast amounts of personal and professional data as well as access to sensitive features such as banking and financial apps. As such protecting our smartphones from unauthorised access is of great importance, and users prioritise this over protecting their devices against digital security threats. Previous research has explored user experiences of unauthorised access to their smartphone – though the vast majority of these cases involve an attacker who is known to the user and knows an unlock code for the device. We presented 374 participants with a scenario concerning the loss of their smartphone in a public place. Participants were allocated to one of 3 scenario groups where a different unknown individual with malicious intentions finds the device and attempts to gain access to its contents. After exposure, we ask participants to envision a case where someone they know has a similar opportunity to attempt to gain access to their smartphone. We compare these instances with respect to differences in the motivations of the attacker, their skills and their knowledge of the user. We find that participants underestimate how commonly people who know them may be able to guess their PIN and overestimate the extent to which smartphones can be 'hacked into'. We discuss how concerns over the severity of an attack may cloud perceptions of its likelihood of success, potentially leading users to underestimate the likelihood of unauthorised access occurring from known attackers who can utilize personal knowledge to guess unlock codes.

CCS CONCEPTS • Security and privacy ~ Human and societal aspects of security and privacy ~ Usability in security and privacy • Security and privacy ~ Human and societal aspects of security and privacy ~ Social aspects of security and privacy • Security and privacy ~ Security services ~ Authentication

Additional Keywords and Phrases: Smartphones, Cybersecurity, Unauthorised Access, Authentication, PIN Codes

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 have become a major part of society following a boom in uptake in the 2010's. The majority of adults in developed economies now own a smartphone [29] and a significant proportion of users claim they could not live without them [22]. As smartphones became widely used by the general public, issues of cybersecurity have become a prominent topic of research. From early on in this body of literature, physical aspects of security relating to the smartphone (i.e., preventing unauthorised access, avoiding loss/theft) have been a prevalent concern to users [8]. This concern over physical security is certainly valid, given the portability of smartphones, and use in public settings where loss or theft are real possibilities [28]. Research has addressed several aspects of physical security, with a major topic being authentication – specifically, the different methods of unlocking smartphones. In the past, many users (~40%) would choose not to lock their smartphone, citing a lack of sensitive data to protect on the device [9], however, currently, smartphones are often used for sensitive tasks; particularly online shopping and mobile banking [13, 19]. More recent work reflects that increased adoption of locking mechanisms has followed the trend of using smartphones for sensitive tasks, with 89% of users now using a lock [16].

However, while lock adoption is high, users do not always choose passcodes (e.g., PINs or swipe patterns) that are robust. Users often choose simple and guessable unlock codes, even when forced to create longer (and theoretically more secure) PINs [20] and swipe patterns [1]. A logical reason for this, is that simpler codes are easier and more convenient to use; previous research suggests that users unlock their phone numerous times in a day, and often in 'safe' situations where a lock is perceived as unnecessary [14] – introducing a trade-off between usability and security in the minds of users.

To better understand how users perceive and engage with locking mechanisms, we can explore how users perceive the nature of attacks and unauthorised usage of their smartphone, which is ultimately the reason locks are employed. In this study, we present 374 participants with an online survey which details a 'lost smartphone' scenario, in which they lose their smartphone in public, and it is found by a stranger who tries to gain access. Participants are allocated to one of three groups, where the unknown individual is presented as having a different level of technical skill and expertise. We ask participants questions about the likelihood of this attack succeeding, how they expect it to be carried out, and the possible outcomes of such an attack. After this, we ask participants to imagine a similar attack by someone they know, allowing us to make comparisons between threat perceptions relating to known and unknown attackers. Our research questions are:

- How do users perceive the nature of unauthorised-access threats to their smartphone? Specifically, how and why do they think these attacks take place, and does this differ for known and unknown attackers?
- How do users rate the likelihood of an unauthorised attack on their smartphone succeeding? How does the threat perception differ based on the identity of the attacker, even within the known and unknown groupings?

Our findings contribute the following:

1. A discussion of how users expect unauthorised access attacks to be carried out against their device. We find that users underestimate the extent to which people who know them may be able to guess their PIN, and overestimate the ability of unknown attackers to use tools to breach their locked smartphone. Combined, we propose how these perceptions could be addressed to support stronger passcode adoption.
- An analysis of how users assess the threat of unauthorised access using Protection Motivation Theory constructs, showing that users are biased in how they weight the severity of an attack from an unknown attacker, and overestimate the likelihood of such attacks actually being successful.

2 Related work

2.1 Perceptions of locking mechanisms

As mentioned above, adoption of smartphone locking is widespread, but there are still issues around perceptions of efficacy and convenience to be explored. Ben-Asher et al. found that users perceived PIN codes, to be insufficient protection for sensitive data stored on the smartphone [4]. Additionally, a field study of phone authentication showed that unlocking represented a small, but non-negligible percentage of the total time spent using the smartphone – on average, 3%, but up to 9% for some users [14]. Importantly, they found many instances of unlocking were conducted in safe settings where a lock felt unnecessary, which may negatively influence users' engagement with locking mechanisms. Where locking methods are perceived as inconvenient, users may be inclined to select less secure PINs, such as their year of birth, or PINs which form a memorable pattern on the keypad [5, 6, 16, 20]. These PINs can easily be guessed by attackers, and people who know the individual can use basic personal knowledge to inform guesses of their unlock code. More complex PINs, and other user-chosen codes such as swipe patterns on Android [1] are important to avoid them being 'guessable', but also to minimise their vulnerability to shoulder surfing [2], where an individual surreptitiously observes a user enter their PIN (or other sensitive information), so they may utilise it later, such as after pickpocketing the phone.

Biometric locks offer more efficient unlocking methods. Initial research on the usability of biometrics has indicated that users often find these methods to be socially awkward in public places, especially face recognition which users describe as feeling like they are 'taking selfies all day' [15]. This may be an issue for some users, but advancements in the technology since this study was carried out in 2015 are likely to mean that users need to make less deliberate gestures to capture their face and can use it without drawing attention to themselves. While biometrics may offer more secure and usable locking options, users still need to setup a non-biometric option as a fallback for when biometrics are unavailable [26, 27] – meaning that user engagement with PINs and Pattern unlocks remain an important issue.

2.2 Unauthorised access: the role of 'known' attackers

To understand the way users are motivated to engage with stronger unlock codes for their smartphone, it is valuable to understand the nature of threats that passcodes are intended to protect against: unauthorised access. Several studies have explored cases where users have experienced unauthorised access; typically this is carried out by people known to the user [17, 18]. Friends, family or partners may often have opportunities to access a user's smartphone. Their proximity to the user may afford them opportunities to 'shoulder surf' a PIN or swipe pattern, or their relationship may even mean they are explicitly told the unlock code, as a gesture of trust [17]. Known attackers are likely candidates to breach a users' smartphone, with over 30% of Marques et al.'s [18] participants admitting to having looked through someone's phone without their permission. Muslukhov [21] dubs these attacks as equivalent to the 'insider attacks' faced by organisations.

The findings of these studies indicate that the nature of these attacks is somewhat different to a typical security threat, as the bad actor in these situations is often socially motivated. Marques et al. [17] explore real instances of unauthorised access from known attackers. These socially motivated attacks are prevalent in romantic relationships, where a lack of trust drives the bad actor to breach the privacy of their partner. Interestingly, findings by [17] also indicate that the more distant the relationship between the bad actor and victim (i.e. friends or colleagues, as opposed to family or romantic partners), the more likely the motive is financial. This suggests that the role of the bad actor may affect the nature of the attack, thus more focus on unauthorised access in a broader range of contexts is necessary to fully understand this issue.

2.3 Lost Smartphones and unauthorised access from unknown attackers

Exploring real cases of unauthorised access outside of known attacker situations is challenging, as these cases would likely only occur when the phone is lost or stolen, and the user wouldn't necessarily know if and how the device was accessed, even if it was returned to them. In place of this, field research by Symantec has offered insight

into the fate of lost smartphones [33]. They used remote monitoring software to observe 50 'lost' smartphones which were purposefully left in public places across the United States. The devices were unlocked, with different apps and folders named to suggest that they held sensitive personal and professional data. They found that only 50% of the devices were returned, and that in most cases, the person who found the device attempted to access data on the phone. 89% of finders accessed personal data, 83% accessed corporate data, 57% tried to open a 'passwords' folder and 43% tried to access the banking app. This study indicates that individuals who find a lost smartphone may often act maliciously and access data beyond what is needed to return the device. As malicious actions from people who find lost smartphone appear to be plausible, this suggests that using lost smartphone scenarios are a valid context to explore unauthorised access through.

Some studies have also addressed how users cope with a lost smartphone. Tu and colleagues [32] used Protection Motivation Theory (PMT) [24] to explain how users would view and cope with a lost/stolen smartphone. They find that an individual's knowledge of the technical responses in relation to a lost/stolen smartphone has a significant influence on their coping appraisal (e.g. using remote access services to locate or wipe the device). To build on these findings, we incorporate questions about the role of remote access features in our survey.

2.4 The reality of breaching smartphone locks

An underexplored dimension of unauthorised smartphone access is the extent to which users believe that attackers could 'defeat' their locking mechanisms, as the above research discusses smartphones that are unlocked, or an attacker who knows an unlock code already [17, 18, 33]. In this section we discuss the practicality of how smartphone locks may be bypassed. If a bad actor has no knowledge of the victim, or opportunity to observe their unlock code, a 'Smudge Attack' can allow an attacker to use marks/fingerprint left on the device's touch screen, to determine a swipe pattern, or the digits used in a PIN previously entered by the user [3]. Under certain conditions, these attacks can be highly successful, albeit requiring a sophisticated lighting and camera setup [3]. Another option is shoulder surfing, in which an individual observes a user entering their unlock code, where it may be later used if they were to gain physical access to the phone. Research indicates that shoulder surfing occurs against smartphone users in public (e.g., public transport, bars and cafes), as well as in private, including the home and workplace [25]. Shoulder surfing can be highly successful; simple pattern unlocks can be memorised with a 64% success rate from a single observation of the code entry [2]. PIN locks appeared to be the most resistant to shoulder surfing, with a 6-digit pin being successfully identified in just 10% of first observations [2].

Alternatively, technical methods of gaining access to a locked smartphone exist, but these are complicated and rely on exclusive technology, as evidenced by high profile court cases in which law enforcement agencies demanded that 'backdoors' be built into smartphones, which would allow them to gain access to suspects' phones [30]. Such cases demonstrate that 'cracking' smartphones is not a simple task and that tools to do so are not readily available, even to major government agencies with substantial resources and expertise. Private companies such as Grayshift and Cellebrite offer services to extract encrypted data from smartphones [7, 12], however these services are offered exclusively to government agencies and law enforcement. For regular bad actors, open-source methods exist, but are not necessarily practical. Android devices have been demonstrated to be vulnerable to Human Interface Device (HID) attacks, in which the phone is plugged into a device which simulates the entry of passwords/patterns until the correct one is determined [23]. Analysis of such attacks indicate that even simple passwords or patterns may take years to crack, given the built in 'cooldown' which prevents users from attempting to unlock the device for a period of time if incorrect attempts are repeatedly made [23]. Regular users may overestimate the efficacy of these methods due to ubiquitous media depictions of 'hackers' forcing access to systems and devices [10].

This study builds the above research to explore how users perceive the efficacy of smartphone locking mechanisms against an attacker who aims to defeat the lock (i.e., not utilizing personal knowledge or shoulder surfing to gain access). Insights from these findings will provide more information about misconceptions that can be addressed to positively influence users to engage with locking methods, particularly stronger authentication choices, such as longer and more complex PINs/patterns that would better protect them from unauthorised access.

3 Method

3.1 Design

The study employed an independent measures design with 3 conditions. The 3 conditions differed in the description of the 'bad actor' in a hypothetical scenario in which the participant loses their phone and it is found by a stranger. The description differed between conditions in terms of the implied skill level and professional background of the stranger.

3.1.1 The lost smartphone scenarios:

The scenarios were developed by the researchers to describe plausible everyday situations in which smartphones may be lost in public and found by a bad actor, similar to the type of places smartphones were 'lost' by researchers in the 'Honey stick Project' [33]. As users may expect that skills or expertise may be involved in breaching/unlocking their phone, we created multiple scenarios that would allow us to explore how the skills level of the attacker may have influenced All three scenarios began with the same base context:

"You visit a café one afternoon, but as you leave, you forget to pick up your smartphone. The next customer who sits at the table discovers your phone and decides they don't want to return it – they will take it home to see what they can access from it."

The latter half of the three scenarios differed, based on the skills/background of the individual who finds the phone. Participants would see only one of the following descriptions:

Scenario 1: The script kiddie

This person has no formal education related to IT or cybersecurity; however, they have always had a strong interest in hacking and spend lots of time reading and watching videos about how to hack smartphones.

Scenario 2: The IT professional

This individual works in the IT department of a large organisation, with a broad set of skills and knowledge around technology, although no specific expertise in hacking.

Scenario 3: The pen-tester

This individual is a skilled computer programmer, and they have previously worked as a 'security tester' where companies paid them to test if their IT systems are hackable.

3.2 Participants

The study recruited 374 participants via Prolific. Participants were aged 18 years or older, and a smartphone user. The sample had an average age of 36.9 years (SD 13.1), ranging between 18 and 89 years. 191 participants were male, 180 were female, 1 non-binary and 2 preferred not to state their gender. 188 were Android users and 186 iOS users. Participants were paid £1.50 for participating. This study was approved by the Psychology department ethics board at Northumbria University, submission reference: 44570.

3.3 Procedure

Participants were presented with an online survey. The survey began by asking for basic demographics (age and gender), followed by details about the smartphone, such as its operating system, manufacturer, and model. Participants were asked about the type of locks they had enabled on their smartphone, and then asked to rate how secure, and how convenient they perceived each type of lock they used to be, using a 5-point Likert scale. After this, they were asked if they used any of the following financial apps on their phone: 'A mobile banking app', 'Shopping apps, which I have saved payment detail in (e.g., card details)' and 'Finance apps, such as PayPal or Revolut'.

3.3.1 Unknown attacker

Participants were then randomly allocated to one of three lost smartphone scenarios. After reading one of the three scenarios, participants were asked about the likelihood of the attacker bypassing locks/unlocking their phone. Next, they are asked about the extent to which the bad actor would be able to access data on their phone. Participants were

also asked how likely the bad actor would be able to spend or transfer their money from the phone. Lastly, participants were asked to indicate what they expected the motivation(s) of the bad actor to be. Participants could select from multiple options but were also asked to specify one primary motivation. After this, we asked participants if they used remote access features on their phone (e.g., find my phone), how they rated their familiarity with these features, and if they could use them to mitigate the success of an unknown attacker, relating to locking the phone, physically reclaiming it, or preventing data being accessed by an attacker.

3.3.2 Known-person comparison.

We then asked participants to imagine a similar scenario, in which someone they know had unsupervised access to their smartphone for an extended amount of time. First, we asked them to state who they expect would be most likely to do so (stating their relationship, e.g., friend, roommate, partner rather than their name). We informed participants we would refer to this person as 'Ash', adapting a naming convention taken from [17]. We asked participants if Ash knows the unlock code for their phone, either from being explicitly told it, or having opportunity to observe it via shoulder surfing. Next, we repeated questions from the earlier scenario; how likely Ash is to bypass their locking mechanisms, to access their data, their finances, as well as Ash's motivations. The final block of questions compared Ash with the stranger. For simplicity, we refer to the stranger as 'Val' – again borrowing the naming convention from [17]. We ask participants who is more likely to gain access to their phone, and who they would be more concerned about gaining access and why this is.

3.4 Analysis:

Analysis was conducted using IBM SPSS V26. Analysis of the three lost smartphone conditions was conducted using one-way ANOVAs. Correlations were measured using Pearson's R. Tests between two groups (e.g., comparing levels of familiarity and use of remote access features between iOS and Android users) were conducted using paired sample t-tests. As we conducted numerous statistical tests, we must control for potential multiple testing problems, where false-positive results may be interpreted as significant. To do this, we applied Holm-Bonferroni sequential corrections, which increase p-values based on the number of tests conducted. The adjustments were made using a tool developed by Justin Gaetano [11]. To ensure data quality, the study included two 'attention check' questions embedded within separate blocks of Likert scale questions at approximately a third, and two thirds through the survey. In place of a statement which participants would respond to, there was an instruction to select a specific option. If participants failed these checks, they were excluded from the study. 9 participants were excluded on this basis.

4 Results:

After receiving data from 100 participants, we paused data collection to conduct a pilot data analysis. After this pilot, three new questions were added to supplement how we measured certain variables, meaning analysis of these variables is based on the following 'main' sample of 274 participants. All other data is based on the full sample of 374 people. The three added questions asked participants to rate: 1. The security and convenience of all smartphone locking mechanisms, whereas we previously only asked them to rate this for the mechanisms that they personally used. 2. Expanding on the previous question, we asked if the factor of security, convenience or trying to balance the two was more influential on participants 3. Lastly, we determined that there may be variability within the same types of relationship (e.g. friend, sibling), so we added questions to measure how close their relationship with Ash was, and how frequently Ash would have an opportunity to access their smartphone.

4.1 Smartphone demographics

188 participants were Android users and 186 were IOS users. Manufacturers were 186 Apple, 95 Samsung, 25 Huawei, 18 Google, 18 Oppo/OnePlus, 10 Motorola, 6 Xiaomi, 5 Nokia, and 13 'other' manufacturers.

22% of smartphones were less than a year old, 36% were 1-2 years old, 23% were 2-3 years old, 11% were 3-4 years old, 5% were 4-5 years old and 3% were over 5 years old. 85% of the sample bought their phone new. 98% of phones in the sample were still supported by software updates. Only 22% of phones in the sample were insured.

4.2 Lock usage and perceptions

Table 1 shows the usage of the seven lock types, alongside a mean rating of their perceived level of security afforded by the lock, and the perceived convenience of using the lock to access the device, both measured on a 5-point Likert scale (a higher score indicates higher security/convenience).

Lock type	N (%)	Security (SD)	Convenience (SD)
PIN	250 (67)	3.77 (.76)	3.42 (.97)
Face Recognition	150 (40)	4.29 (.90)	4.07 (1.2)
Fingerprint	148 (40)	4.58 (.67)	4.32 (.91)
Swipe pattern	39 (10)	3.2 (1.01)	3.25 (1.1)
Password	36 (10)	3.96 (.78)	2.77(1.1)
No lock	15 (4)	1.13 (.52)	4.65 (.78)
Iris	4 (1)	4.49 (.79)	3.90 (1.1)

Table 1: Usage and perceptions of different lock types

A PIN lock was most common, however, the majority of the sample used more than one locking mechanism. 182 participants (49%) used 2 locking types, and 11% used 3 or more locking types. Typically, participants used a PIN lock in conjunction with a form of biometric lock, most likely a result of biometric methods requiring a 'fallback' non-biometric method to be in place – just 72 participants used a PIN without also having a biometric method in place, indicating the prevalence of PINs is largely due to being necessary as a backup when enabling biometric methods. Fingerprint unlocking was rated as the most secure and most convenient method of locking (excluding the 'no lock' option, which was rated as more convenient but also rated as highly insecure).

If we group the lock types as biometric (Face, Fingerprint, and Iris) or non-biometric (PIN, Password, and Pattern) and exclude the 'no-lock' option, the biometric methods were rated as much more secure (4.45, SD .66), then the non-biometric methods (3.64, SD .63). A paired samples t-test indicates the difference is significant *(t(276) =15.450, p = <.000)*. Similarly, the biometric mechanisms were seen as significantly more convenient (4.09, SD.94) than the non-biometric mechanisms (3.14, SD .83); *(t(277)= -13.442, p=<.000)*. Additionally, the age of participants appeared to influence perceptions of lock types. Age correlated positively with the perceptions of how secure biometric locking mechanisms are (*r=.159, p=.049*), but there was no significant correlation between convenience and age (*r= -.149, p=.065*).

Finally, we asked which mattered more to participants when choosing a lock type, security, or convenience. Participants were given 3 statements; 'I try to choose the most [secure/convenient] option' and 'I try to balance security and convenience'. 191 (69%) participants tried to balance the two, 46 (17%) prioritised security and 39 (14%) prioritised convenience. As biometric mechanisms appear superior in both attributes, this likely means participants do not view security and convenience as mutually exclusive and can achieve both together.

4.3 The Lost Smartphone Scenarios

Participants were asked to rate how likely the bad actor in the lost smartphone scenario would be to bypass the locking mechanisms of their smartphone. This was measured using 3 different statements and a 5-point Likert scale, from 1 (strongly disagree) to 5 (strongly agree). The results are shown in Table 2. As a reminder, Condition 1 was the novice hacking enthusiast, Condition 2 was the IT specialist, and Condition 3 was the security expert.

Statement	Cond. 1 (SD)	Cond. 2 (SD)	Cond. 3 (SD)
The locking mechanisms would prevent the person from being able to unlock my phone	3.44 (1.1)	3.56 (1.2)	2.73 (1.2)
They would be able to find tools or information online that would allow them to unlock my phone	3.75 (1.0)	3.5 (1.1)	3.75 (1.1)

They would be able to figure out a way to unlock my phone	3.46 (1.1)	3.32 (1.1)	3.83 (1.0)

Table 2: The mean rating for each attacker's likelihood of unlocking the phone.

A one-way ANOVA suggests a significant difference between conditions: (f(2,371)= 18.6), p=<.016) for the efficacy of the locking mechanism, with the locking mechanisms being most likely to fail against condition 3's attacker - the security professional. A one-way ANOVA also suggests significant difference (*F(2,371)=7.7), p=<0.016*) in ability to figure out how to unlock a phone, again with condition 3 most likely. However, a one-way ANOVA found no significant difference between the conditions (*F(2,371=1.149), p=.600*) for ability to find tools to unlock the phone. This indicates that participants perceive the attackers as equally likely to find tools that would assist in unlocking the device, yet the security professional (condition 3) would be more successful overall.

When asked to rate the likelihood of the bad actor bypassing a specific lock-type using a five-point Likert scale, where a higher score is more likely to be bypassed. A one-way Anova (*F(2,247=3.082), p=.032*) found only one significant difference between conditions was found; the security professional (condition 3) would be more successful at defeating PIN locks, with a mean rating of 3.72, compared to ratings of 3.33 and 3.14 for conditions 1 and 2.

Biometric locks were rated as much less likely to be breached by any of the 3 attackers (2.1, SD 1.06) than non-biometric locks (3.4, SD 1.16). A further one-way ANOVA found no significant difference between conditions in regards to bypassing biometric (*F(2,308=2.351), p=.291*) or non-biometric (*F(2,263=.852), p=.600*) locks, suggesting the cause of the difference is the locking mechanisms and not the differing attacker conditions.

4.4 Methods of gaining access

In response to an optional open question about how the unknown-attacker, Val, might have succeeded in accessing the phone, 186 participants gave valid responses which were manually coded into 10 different categories, shown below in table 3, including how many participants answered in each category and their % of the responding group.

Method	Definition	N(%)
Software	Using software designed to either bypass the locks, determine the pin, or provide access without doing either. Several suggestions that this was paid or 'hacker' software, indicating some level of exclusivity.	68(37)
Miscellaneous 'hacking'	Generic responses such as 'hacking the phone', 'hacking the pin' etc.	34(18)
Guessing the PIN code	Trying common pins, random guessing etc.	26(14)
Using online information	Online guides, videos, and forums (sometimes found specifically on the dark web) used for advice and guidance.	22(12)
Tricking biometrics	Using pictures of the owner's face to bypass facial recognition.	9(5)
Resetting the phone	Some, but not all, acknowledged this would mean Val loses the data on the phone	9(5)
It's not possible	These participants felt it was not possible to break into a phone like this, referencing knowledge that there are no 'back-doors' built into smartphones, even for police access.	7(4)
Residue	Using marks on the screen to identify possible PIN or swipe patterns.	6(3)
Third-party help	Taking the phone to a phone shop, repair shop, or other unspecified third party	3(1)
Shoulder-Surfing	Covertly observing an unlock code being entered before taking hold of the device.	2(1)

Table 3: Participant expectations of how their phones could be breached.

Software was the most common response for those who answered, indicating users imagine that the attack occurs through the application of specialist programs. This is furthered by the fact that we found no significant difference between the conditions based on the earlier statement regarding the likelihood of finding tools or information that would let them gain access, indicating any of the attackers could access the same resources. However, as Condition 3 was typically rated as most likely to succeed in gaining access, it appears participants rate them as more competent at utilising software or tools than conditions 1 and 2.

4.5 Data Access

Table 4 shows the extent to which participants felt the bad actor in each condition could access data on their smartphone and make use of it in some way. These statements began with 'They would be able to…'

Statement	Cond. 1 (SD)	Cond. 2 (SD)	Cond. 3 (SD)
Access the data on my phone if they could unlock it	4.33 (.903)	4.40 (.825)	4.51 (.716)
Access the data on the device, even if they could not unlock it*	2.02(1.01)	2.24 (1.164)	2.48 (1.165)
Access personal data that they could use against me*	3.05 (1.109)	2.69 (1.157)	3.26 (1.202)

Table 4: Average responses to statements about the attacker gaining access to data and services on the device. *significant difference between conditions for these statements.

The significant difference between responses for statements 1 and 2 across the full sample (*t(373) = 30.176, p=<.000)* provide insight to participants' awareness of how their data can be accessed. While the response to statement 1 may seem self-evident - that attackers could access data if they could unlock the device, when compared to the responses to statement 2, we see that participants understand that unlocking the phone is central to accessing the data on their phone; it can't simply be extracted, such as by plugging it into a computer.

Next, we asked participants about financial apps and data on their phone. Table 5 below shows the prevalence of these apps and data types.

App/Data Type	N(%)
Mobile Banking App	336 (90)
Shopping app with saved payment details	284 (76)
Finance Apps (e.g. Paypal, Revolut)	293 (78)
Documents containing financial info and details	80 (21)
Notes saved containing financial info and details	77 (21)
None of the above	0

Table 5: Prevalence of financial apps and data used by the sample

Financial apps and data are highly prevalent in our sample - no participants selected the 'none of the above' option. We build on this data by asking participants about the likelihood of financial damages occurring as a result of the scenario, the results of which can be seen in table 6 below. We only include data from participants who have the applicable data/app types. Statement 1: only participants who had 1 or more of a banking app, shopping app with saved payment details, **or** other finance apps (n=355). Statement 2: only participants who have a mobile banking app (n=336). Statement 3: only participants who have an 'other' finance app installed (n=293). Statements are scored from 1 (strongly disagree) to 5 (strongly agree) and began with 'the person who has my smartphone would be able to use it …'.

Statement	Cond. 1 (SD)	Cond. 2 (SD)	Cond. 3 (SD)
… to use it to spend my money	3.15 (1.4)	3.30 (1.4)	3.68 (1.2)
… to use it to transfer money from my bank account	2.58 (1.4)	2.63 (1.4)	3.27 (1.4)

... to transfer money from other finance/payment apps such as Paypal, Revolut or investment apps	2.86 (1.4)	2.86 (1.4)	3.46 (1.4)

Table 6: Average responses to statements about the attacker making financial gain from the smartphone.

Condition 3's security professional was rated as significantly more likely to make financial gains than the other two bad actors across all three statements. They were more likely to; spend money using the smartphone (*F(2,352=5.041), p=.049*), transfer money from the participants' bank account (*F(2,333=6.104), p=.020*) and transfer money from finance/payment apps (*F(2,292=6.378), p=.020*). The most substantial difference is for statements 2 and 3, where attacker 3 is substantially more likely to succeed in making financial gain by accessing financial/banking apps on the smartphone.

We concluded questions about the lost smartphone scenario by asking participants to rate how likely they would be to lose their phone in the manner described in the scenario. 24% of participants selected never, 51% selected 'unlikely'. 22% selected 'It's a possibility', 3% selected 'likely', and less than 1% selected 'very likely'.

4.6 Remote access services

We asked participants about using remote access services to respond to the lost phone scenario. In total, 293 participants reported having a remote access service enabled on their phone; these were primarily Apple's Find my iPhone, Samsung's Find my Mobile, and Android's Find my Device, all of which have comparable features. After setup, 53% of Android users had accessed their remote access service before compared to 65% of IOS users. Participants rated several statements about using remote access features using 5-point Likert scales, and results are shown in table 7 below with the average ratings.

Statement	Avg. (SD)	Correlation with familiarity
How familiar are you with the remote access settings on your smartphone?	3.04 (1.35)	-
I could easily access another device to remotely track, access or control my phone on	3.84 (1.11)	.389
I would be able to prevent the person who has my phone from unlocking it	3.24 (1.09)	.352
I would be able to prevent the person who has my phone from accessing the data on it	3.27 (1.13)	.373
I would try to get my phone back from the person using the location tracking feature	3.99 (1.00)	.219
I would be able to copy data from my phone remotely, so I don't lose anything	3.30 (1.12)	.312

Table 7: Average ratings of the remote access statements, and their correlation with participant familiarity. All correlations were significant at p= <.01

We observed that familiarity with the features of the remote access service correlated significantly with every other statement; indicating familiarity with the features is an important factor in understanding their role in a lost/stolen phone situation. This is important as unfamiliar users may be unaware of important options for protecting their data if the phone is stolen, such as remotely backing up and wiping the device. iOS users rated their familiarity with remote access features significantly higher than Android users (*t(291)= -9.732, p=.016*). We found no other significant differences based on OS, and no differences between unknown attacker conditions for any of the remote access statements.

4.7 The Insider-Attack Scenario

For the latter part of the study, participants were asked to imagine someone they know trying to gain access to their phone, at a time when they left the device unsupervised. First, we asked participants to express who this person

was, based on their relationship to them. This question used an open response text box and we coded responses into one of eight categories. This individual would be referred to as 'Ash' for the rest of the study, again borrowing a naming convention from [17]. Table 8 below shows the frequency of each category and how we coded them, alongside how close participants rated their relationship, and how likely they believe the individual would have an opportunity to access their smartphone, both of which were measured using 5-point Likert scales – a higher score indicates greater closeness, and a higher frequency of opportunity.

Category	Coding	N(%)	Closeness	Opportunity
Partner	Romantic partners ('boyfriend', 'wife' etc.).	111 (30)	4.5	3.8
Friend	Friends, often written with contextual indicators ('old friend', 'friend from the pub')	101 (27)	3.1	2.5
Colleague	Colleagues and other relationships with a professional basis ('student', 'coach')	60 (16)	2.2	2.3
Close relative	Immediate family (parents, children, siblings)	41 (11)	4.4	3.1
Unspecified	responses of multiple individuals, or an undefined individual (e.g., 'either a colleague or partner', 'someone random from uni')	26 (7)	3.1	1.2
Acquaintance	People who are known but not close, e.g., neighbour, friend of a friend	14 (4)	1.4	2.0
Relative	Non-immediate family (cousins, niece/nephews, in-laws)	12 (3)	3.4	2.5
Roommate	Cohabiting individuals who aren't a partner or close relative	9 (2)	3.3	2.4

Table 8: The prevalence of different categories of Ash's identity

The closeness of the relationship correlates significantly with the frequency of opportunity to gain access ($r(273)= .58, p=<.000$). The average rating of Ash's opportunity to access the phone is 2.84 (SD 1.3) and the average likelihood of the phone being available to bad actors such as Val (i.e. lost in public), is 2.06 (SD .8). A two-tailed paired samples t-test reveals there is a significant difference between the variables ($t(276) = -8.690, p=.016$), supporting that known attackers have greater frequency of opportunities to access users' devices.

We asked participants if Ash knew an unlock code for their phone. Participants could answer that they had explicitly told Ash the code, if they believed Ash knew it through observing/shoulder surfing, if they were confident Ash did not know the code, or if they were unsure whether Ash knew it. Table 9 below summarises these responses for each category of Ash.

Category	Told code %	Seen code%	Does not know %	Unsure %
Partner	53 (48)	22 (18)	23 (21)	13 (12)
Friend	9 (9)	9 (9)	74 (73)	9 (9)
Close relative	10 (24)	7 (17)	20 (49)	4 (10)
Colleague	0	1 (2)	56 (93)	3 (5)
Acquaintance	0	1 (7)	11 (79)	2 (14)
Relative	1 (8)	0	11 (92)	0
Unspecified	3 (12)	1 (4)	21 (81)	1 (4)
Roommate	2 (22)	0	7 (78)	0

Table 9: Participants reports of whether Ash knows an unlock code for their phone

Additionally, 7 participants indicated Ash had their biometrics registered to unlock the phone (5 partners, 1 each of friends and close relatives). 8 participants were unsure if Ash had their biometrics registered (2 each of partners, friends and roommates, and 1 each of colleagues and acquaintances). Overall, 60% are confident Ash does *not* know an unlock code. 21% have explicitly told Ash an unlock code and 11% are confident Ash has seen them enter an unlock code enough to know it. This means Ash knows an unlock code in 32% of cases, with up to an additional 8% who are unsure if Ash knows an unlock code. Of the 119 cases where participants told Ash an unlock code, or are confident they have observed it, Ash is a romantic partner in 63% of these cases.

4.7.1 Ash's motivation

We asked participants to select what they expected to be Ash's motivations. The following options were chosen by participants; curiosity (58%), followed by financial gain (22%), were the most prevalent options, representing Ash's motive in the majority of cases (80%). The next most common motivation was 'Accessing data to use against me' (13%), followed by 'as a challenge to themselves' (4%). For participants who selected the 'other' option (4%), they were able to specify the motive they expected – these responses indicated harmless motives, such as using the phone for a functional reason (e.g., searching something online while the device is at hand), or for positive reasons such as 'arranging a surprise party'.

In figure 1 below, we explore how the expected motivation changes in relation to how close participants rate Ash (on a 1-5 scale). There is a clear trend where more distant relationships associate with financial motivations, but closer relationships appear to be more socially motivated, supporting the idea that unauthorised access from close individuals, more well-known to the user, typically represents a privacy/trust breach, while unauthorised access from strangers or more distant known persons is more of a security breach with tangible bad outcomes, such as financial losses.

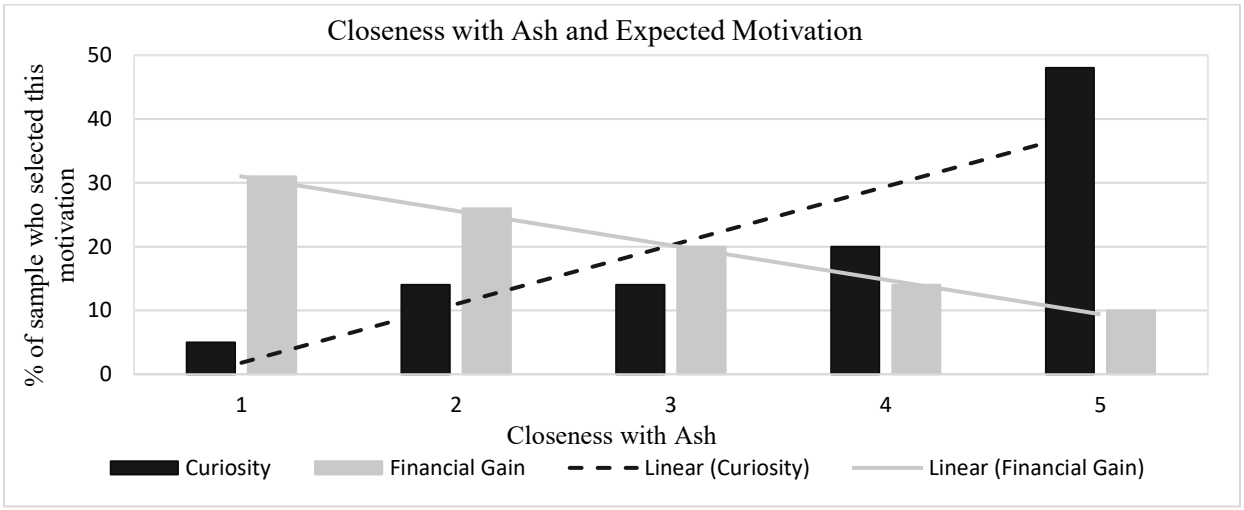

Figure 1: Comparing closeness, and prevalence of financial gain and curiosity motivations

4.8 Comparing Ash and Val

71% of participants said Val is more likely to succeed in gaining access to their smartphone and 29% expected that Ash would be more likely to succeed. This is despite Ash knowing the code in between 32-40% of cases, as well as the factor of personal knowledge that could be used to guess an unlock code (e.g. a year of birth used as a PIN [5, 6, 16, 20]). Beyond those who explicitly know an unlock code, there is likely to be a greater proportion of known attackers who could gain access compared to what participants expect.

An exception to Val being viewed as more likely to succeed at gaining access is when Ash was imagined to be the participants' partner, when 56% of participants expect Ash to be more likely to succeed. This is probably due to partners being the most likely group to know an unlock code for the smartphone, however, there is still a substantial number of participants for whom Ash knows the code, but still view Val as more likely to gain access, suggesting users underestimate the value of personal knowledge in guessing their unlock codes. This perception is likely tied to the expectation of unauthorised access being facilitated by technical skill rather than personal knowledge; Val was rated as significantly more proficient, in both general technical skills ($t(373)=19.541, p=.016$) and skill at gaining access to a locked device ($t(373)=21.489, p=.016$) than Ash.

Perhaps unsurprisingly, 70% of participants say they are more concerned by Val trying to gain access to their phone than Ash. Participants were given an optional open-response box to explain their choice. We coded these responses into 4 categories; 1: based on expected motive/outcome of the attack (n=126), 2: based on the likelihood of success (n=59), 3: based on trust/loyalty from Ash, or a lack of this from Val (n= 105), 4: unclear/no response (81). Motive/outcome related reasons were most common, where the likelihood of success was rarely considered. Motive/outcome focused explanations typically reference Val attempting to gain financially: *"Val would probably steal my money and could steal my identity. Ash wouldn't, and would just want to look at messages" (P154).* Where Ash's motives were referenced, they were usually social; *"Because [Ash] would just be curious, checking for infidelity etc. (P61).* Participants appeared to view the financial losses as more damaging than whatever Ash may find or do; *"Financial losses are more stressful than mild embarrassment"* (P261). Knowing the bad actor and anticipating the nature of an attack from them seemed to reduce the threat perception of participants; *"Better the devil you know!" (P368).*

5 Discussion

We used scenarios to explore participants' perceptions of lost smartphones and unauthorised access. Presenting participants with situations in which a stranger, or someone they know attempts to gain access to their smartphone provides us with several insights in relation to their perceptions of their smartphone's lock efficacy, attacker motivations, threat severity, and threat vulnerability. Lastly, we discuss how participants perceive the nature of successful attacks from an unknown attacker and consider the feasibility of these attacks in relation to participants' expectations.

5.1 Weighing up motivation, ability and opportunity

When asking participants to weigh up the risks of unauthorised access from a known actor, versus from an unknown actor, several factors appeared to influence their perceptions. Importantly, the motivation behind the attack appeared to outweigh the likelihood of it even succeeding. To understand how participants assess these threats, we use constructs from Protection Motivation Theory (PMT) [24], a model that is often used to measure how users assess security threats [31, 32].

5.1.1 Threat Vulnerability

In the context of this study, we treat the 'threat vulnerability' factor of PMT as the likelihood that the bad actor can gain access to the phone. This relies on having opportunities to take hold of the phone, and the knowledge or ability to unlock the device. Known attackers have more opportunities to take hold of the device, as they can take advantage of situations when the smartphone is left unattended in shared spaces. In contrast, participants rated the likelihood of them losing their smartphone in the way the first scenarios describe as somewhat unlikely – making it rare for them to be exposed to an attack by an unknown attacker like Val. We found that the opportunity for Ash to access the device correlated significantly with the users' closeness with Ash, which supports previous findings that the people closest to us (e.g. partners and close friends) have the most opportunity to gain access to our devices [18].

We also view the likelihood of the device being unlocked by the attacker as part of the 'threat vulnerability' factor. Most participants expected Val would be most likely to unlock their smartphone: only 29% of participants expected Ash would be more likely to gain access, a similar figure to the number of participants who believed Ash knew their unlock code (from sharing it with Ash, or them having seen it entered frequently). While these two data points align, this means that participants are likely underestimating the extent to which people close to them can utilise personal

knowledge to make more educated guesses to their phone's unlock codes – especially as users often choose PINs based on personal details such as their year of birth [5, 6, 16, 20]. Future research could explore how guessable users expect their PIN to be by other individuals; again considering different levels of closeness. Users could also be challenged to guess the PINs of other people they know, which may help demonstrate that common, simple PINs based on personal details can be easily guessed, potentially motivating users to choose more complex PINs.

5.1.2 Threat severity

We treat the 'Threat Severity' factor of PMT as the outcome of the attack; what the bad actor does with the device and any data/features they can access. Ash's social motivations seem largely harmless to participants, while Val's financial motivations are quite damaging, meaning the threat severity from unknown bad actors is much higher. Despite unknown bad actors having much lower opportunity to access the device, participants still indicated being more concerned about these attacks, often citing the more severe, financial motivations of this attack. This is an important characteristic for understanding the threat appraisal of users, as the weighting appears highly skewed towards the severity of the threat, with little consideration of how vulnerable users truly are. Interventions to address inaccuracies in these perceptions may play a role in encouraging engagement with strong PINs.

Another consideration around the severity of access from known bad actors, is the potential for domestic abuse, as smartphones have been established as a medium through which abusers control and monitor victims [34]. While 'snooping' or checking for infidelity may be one-off acts of mistrust, they may represent a more malicious and recurring pattern of behaviour from abusive partners. Only one participant indicated that personal abuse was their reason for selecting Ash as a greater threat, though they earlier indicated that they imagined Ash as a close relative. So, whilst the majority of our sample view the threat of Ash as benign, known attackers should not be sweepingly deemed as insignificant, as for other individuals, a known attacker may leverage access as a means of abuse, and utilise this access for ongoing violations, such as installing 'stalkerware' applications that covertly record the victims' location and activities, feeding this information back to the abuser. Alternatively, known attackers may use knowledge of the phone's unlock code to reveal login details for other services/accounts (via password managers which may reveal saved passwords if the phone's unlock code is provided). This could allow an attacker even broader access which they can revisit without having access to the phone, and could continue for extensive periods of time, including after breakups in intimate partner relationships.

5.1.3 Coping appraisal

In PMT, the coping appraisal encompasses response efficacy – the extent to which users feel the available countermeasures can help them remedy the situation, and self-efficacy, their ability to enact responses and personally deal with the situation. In this context, response efficacy refers to the use of remote access features (e.g. 'find my phone') to mitigate the consequences of losing their smartphone, by tracking its location, preventing it from being unlocked, and backing up and wiping it's data. We found that individuals less familiar with remote access features overall would feel less able to recover their phone and less able to mitigate the consequences of it being lost. As iPhone users are more familiar with remote access features, they may be better placed to cope with and respond to a lost smartphone. Android developers or manufacturers such as Samsung may consider more explicitly encouraging and supporting their users in setting up and familiarising themselves with remote access features.

5.2 Lock perceptions and methods of 'breaking in'

We found that participants largely viewed biometric unlocking methods as highly secure and convenient, especially in comparison to non-biometric methods such as PINs and patterns. This applied as a general perception of the level of security offered, but also when applied to the lost smartphone scenarios, as participants viewed the PIN unlock as most likely to be defeated by an attacker. This perception is realistic to an extent, as non-biometric locks are theoretically vulnerable to brute force attacks from Human Interface Devices [23] – though these attacks may take years to succeed. While participant concerns about the use of these tools is inflated, it is true that code-based unlocks are the most exploitable, especially considering more realistic methods like shoulder surfing. As our data showed that participants viewed biometrics as both the most secure and convenient unlocking methods, developers could consider reducing the need for code based unlocks as a backup method, as these undermine the security afforded by biometrics.

While some users may frequently be unable to use biometrics, such as due to protective clothing worn for work (glasses, gloves, masks etc.), the average user may not often experience these issues, and feel comfortable to not need an easily inputted backup like a PIN. In this case, backup methods may be better pitched to users as something that would only be relied on rarely, and should be longer and more complex, i.e., a typical password. If developers deem that code unlocks like PINs should remain as a backup for biometrics, then heightening awareness of easily guessable PINs during setup should be prioritized. Displaying information, such as the most common PIN being the users' birth year/birthday, which are easily guessed, may help dissuade users from choosing these PINs. Finally, as familiarity with remote access services appeared to increase a users' ability to cope with a lost smartphone situation, developers should endeavor not just to maximize how many users set up these services, but also to increase exploration of the features. As Android users are less familiar with remote access services, manufacturers and developers in the Android ecosystem should particularly consider taking greater steps to maximise user familiarity with remote access services.

5.3 Limitations

1. We present participants with a very specific lost smartphone scenario, but these attacks may take place under many different settings. Attackers likely would plan the attack, and attempt to shoulder surf an unlock code before taking the device. Thieves may snatch the phone from the user while it is unlocked, allowing them to make contactless/NFC purchases using the phone. A phone may also be stolen alongside things which could inform guesses of a passcode (e.g. an ID card displaying year of birth). These different possibilities are likely to have different outcomes and success rates compared to the scenario we presented to participants.

- When asking participants about the potential for Val to spend their money, we did not ask if participants had their card details saved, to allow the phone to be used for contactless/NFC payments. This may have been an interesting data point, as the phone only has to be unlocked to use this functionality, whereas mobile banking and other financial apps often have their own separate login pages.
- This study largely explores hypotheticals and participant expectations of particular scenarios. While these are valuable in assessing threat perceptions, as these likely influence their behaviour and level of engagement with protective behaviours, they have limited validity in understanding things such as how known attackers may act, as this isn't guaranteed to follow the expectations of victims/our participants.

6 Conclusion

We explored users' perceptions of the security of smartphone authentication methods, alongside their threat perceptions relating to unknown bad actors of varying skill and experience, compared against known individuals who may have existing knowledge of the participants and their devices' unlock codes. Participants view PIN codes as more likely to be bypassed than biometrics, due to an expectation that 'hacking' tools can brute force their PIN code. However, it also appears that participants underestimate the extent to which people close to them could guess their PIN, based on personal knowledge or surreptitious shoulder surfing. We suggest that future research should explore interventions to address these perceptions which may lead to poor PIN choices; guessable PINs that anyone with basic knowledge about the user could exploit.

In line with previous findings [17], we find that users often share their smartphone unlock codes with people they are close to, which open them up to privacy or security violations, even if they trust the individual. Closer individuals are perceived as more likely to engage in privacy violations, but more distant individuals are perceived as more likely to engage in financial attacks if they were able to access the phone. We find that user perceptions of how their phone might be 'hacked' are realistic in nature, but overestimate the efficacy of these methods.

References

<bib id="bib1"><number>[1]</number>1] Aviv, A.J., Budzitowski, D. and Kuber, R. 2015. Is bigger better? Comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock. *ACM International Conference Proceeding Series*. 7-11-Decem, (2015), 301–310. DOI:https://doi.org/10.1145/2818000.2818014.
<bib id="bib2"><number>[2]</number>[2] Aviv, A.J., Davin, J.T., Wolf, F. and Kuber, R. 2017. Towards baselines for shoulder surfing on mobile authentication. *ACM International Conference Proceeding Series* (2017), 486–498.</bib>

<bib id="bib3"><number>[3]</number>[3] Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. and Smith, J.M. 2010. Smudge attacks on smartphone touch screens. *4th USENIX Workshop on Offensive Technologies, WOOT 2010* (2010).</bib>
<bib id="bib4"><number>[4]</number>[4] 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.</bib>
<bib id="bib5"><number>[5]</number>[5] 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.</bib>
<bib id="bib6"><number>[6]</number>[6] 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).</bib>
<bib id="bib7"><number>[7]</number>[7] Cellebrite - Digital Intelligence For A Safer World: *https://cellebrite.com/en/home/*. Accessed: 2023-01-24.</bib>
<bib id="bib8"><number>[8]</number>[8] 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).</bib>
<bib id="bib9"><number>[9]</number>[9] 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.</bib>
<bib id="bib10"><number>[10]</number>[10] Fulton, K.R., Gelles, R., Mckay, A., Roberts, R., Abdi, Y., Mazurek, M.L., Clara, S., Fulton, K.R., Gelles, R., Mckay, A., Roberts, R., Abdi, Y. and Mazurek, M.L. 2019. The Effect of Entertainment Media on Mental Models of Computer Security This paper is included in the Proceedings of the The Effect of Entertainment Media on Mental Models of Computer Security. (2019).</bib>
<bib id="bib11"><number>[11]</number>[11] Gaetano, J. 2018. Holm-Bonferroni sequential correction: An Excel Calculator (1.3).</bib>
<bib id="bib12"><number>[12]</number>[12] GrayKey Cell Phone Forensics Tool: *https://www.grayshift.com/graykey/*. Accessed: 2023-01-24.</bib>
<bib id="bib13"><number>[13]</number>[13] Great Britain: online banking use 2020: 2020. *https://www.statista.com/statistics/286273/internet-banking-penetration-in-great-britain/*. Accessed: 2022-05-09.</bib>
<bib id="bib14"><number>[14]</number>[14] 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.</bib>
<bib id="bib15"><number>[15]</number>[15] 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.</bib>
<bib id="bib16"><number>[16]</number>[16] Markert, P., Bailey, D. V., Golla, M., Durmuth, M. and Avig, A.J. 2020. This PIN can be easily guessed: Analyzing the security of smartphone unlock PINs. *Proceedings - IEEE Symposium on Security and Privacy*. 2020-May, (2020), 286–303. DOI:https://doi.org/10.1109/SP40000.2020.00100.</bib>
<bib id="bib17"><number>[17]</number>[17] 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).</bib>
<bib id="bib18"><number>[18]</number>[18] 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.</bib>
<bib id="bib19"><number>[19]</number>[19] 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.</bib>
<bib id="bib20"><number>[20]</number>[20] 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.</bib>
<bib id="bib21"><number>[21]</number>[21] 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.</bib>
<bib id="bib22"><number>[22]</number>[22] Ofcom 2015. *The Communications Market Report (2015).*</bib>
<bib id="bib23"><number>[23]</number>[23] Potocký, S. and Štulrajter, J. The human interface device (hid) attack on android lock screen non-biometric protections and its computational complexity. *Science & Military*. 1, 2022. DOI:https://doi.org/10.52651/sam.a.2022.1.29-36.</bib>
<bib id="bib24"><number>[24]</number>[24] Rogers, R. and Prentice-Dunn, S. 1997. Protection motivation theory. *Handbook of health behavior research 1: Personal and social determinants*. (1997), 113–132.</bib>
<bib id="bib25"><number>[25]</number>[25] Schneegass, S., Saad, A., Heger, R., Delgado, S., Poguntke, R. and Alt, F. 2022. An Investigation of Shoulder Surfing Attacks on Touch-Based Unlock Events. *Proceedings of the ACM on Human-Computer Interaction*. 6, MHCI (2022). DOI:https://doi.org/10.1145/3546742.</bib>
<bib id="bib26"><number>[26]</number>[26] Set up Touch ID on iPhone: *https://support.apple.com/en-gb/guide/iphone/iph672384a0b/ios*. Accessed: 2023-06-05.</bib>
<bib id="bib27"><number>[27]</number>[27] Setting up the Biometrics and Security: 2022. *https://www.samsung.com/au/support/mobile-devices/setup-biometrics-and-security/*. Accessed: 2023-06-07.</bib>
<bib id="bib28"><number>[28]</number>[28] Smart phone thefts rose to 3.1 million in 2013: 2014. *https://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm*. Accessed: 2022-06-20.</bib>
<bib id="bib29"><number>[29]</number>[29] Taylor, B.Y.K. and Silver, L. 2019. *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally.*</bib>
<bib id="bib30"><number>[30]</number>[30] Thielman, S. 2016. Apple v the FBI: what's the beef, how did we get here and what's at stake? . *The Guardian.*</bib>
<bib id="bib31"><number>[31]</number>[31] 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.</bib>
<bib id="bib32"><number>[32]</number>[32] Tu, Z., Turel, O., Yuan, Y. and Archer, N. 2015. Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information and Management*. 52, 4 (2015), 506–517. DOI:https://doi.org/10.1016/j.im.2015.03.002.</bib>
<bib id="bib33"><number>[33]</number>[33] Wright, S. 2012. The symantec smartphone honey stick project. *Symantec Corporation, Mar.*</bib>

<bib id="bib34"><number>[34]</number>[34] Yardley, E. 2021. Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework. *Violence Against Women*. 27, 10 (2021), 1479–1498. DOI:https://doi.org/10.1177/1077801220947172.</bib>
<bib id="bib35"></bib></bib>