Evolving smartphone usage and the growing threat to consumers

Nuke from orbit | KAM

Contents

Foreword

When we started Nuke From Orbit, it was important to us personally that we establish the scale of the problem we were looking to solve. You can have the best idea in the world, but if there's no market for it, then it's never going to take off.

So, when you commission research like our study into evolving smartphone usage and the growing threat to user security, it's a scary proposition. Because it either proves or disproves your thesis. Data, however, is the lifeblood of any business, so before we launched ourselves into the cold darkness of space (where no one can hear your scream), we wanted certainty – or as much as you can have in an uncertain world – that we'd made the right call.

What we couldn't have predicted was just how right we were. In many cases, the responses exceeded our expectations, and not in a good way. Not only is the number of people who've had a phone stolen staggeringly high, but the aftereffects are varied and highly damaging. As the functionality of smartphones increases and phone thefts proliferate, the risk to individuals increases.

We use our smartphones to bank, shop, communicate, manage businesses, store personal information...the list goes on. Our lives, for better or worse, are intrinsically tied to the little black box in our pocket or handbag. While the security on such devices has evolved since Apple launched the first iPhone in 2007 (we can debate when the first smartphone was launched but this is unequivocally when they went mainstream), so have criminals.

Smartphones are the gateway to a digital world and our digital selves, but they're also the single greatest point of vulnerability. If you can get in someone's phone, you can control their life, and wreak untold havoc on their finances, relationships and reputation.

So, while we work hard to meet these challenges head on, we present to you the findings of our research to better understand how the modern consumer is using their smartphone, and the vulnerabilities this creates.

James O'Sullivan
CEO and Founder, Nuke From Orbit

Introduction

Purpose of research

This research was conducted to understand and quantify the problem of mobile phone theft and the subsequent consequences. This research was also conducted to assess the vulnerability and susceptibility of smartphone users if their phone was stolen, based on current security measures. Finally, the research addresses which services are most important to protect, and assess the appetite for a service that supports device blocking.

Methodology

The research was carried out by KAM on behalf of Nuke From Orbit in August 2023. A nationally representative sample of 1,000 UK adults (18+) with a smartphone were surveyed via an online platform.

If you would like the full research data, please contact marketing@nuke.app

Key Insights

Smartphones are so much more than a communication device with **78% using it for mobile banking** and **51% using it as a digital wallet**.

Despite the associated risks, **45% of us are using the same PIN** for mobile apps as we do to get into our phone and **42% of us are unaware** that this PIN can be used to make payments via digital wallets.

Phones being stolen is not uncommon with **17% of smartphone** users saying it had happened to them. More concerningly is that when the phone was stolen, more often than not, social, communication and financial apps were compromised.

Although there are many security measures in place such as biometrics or password manager, they are **not infallible**, may present a **greater risk if accessed** and become **redundant** if the thief has certain information.

Three in four smartphone users would be interested in a service that allows them to block services accessible through their smartphone after theft, with the financial services the most important to protect.

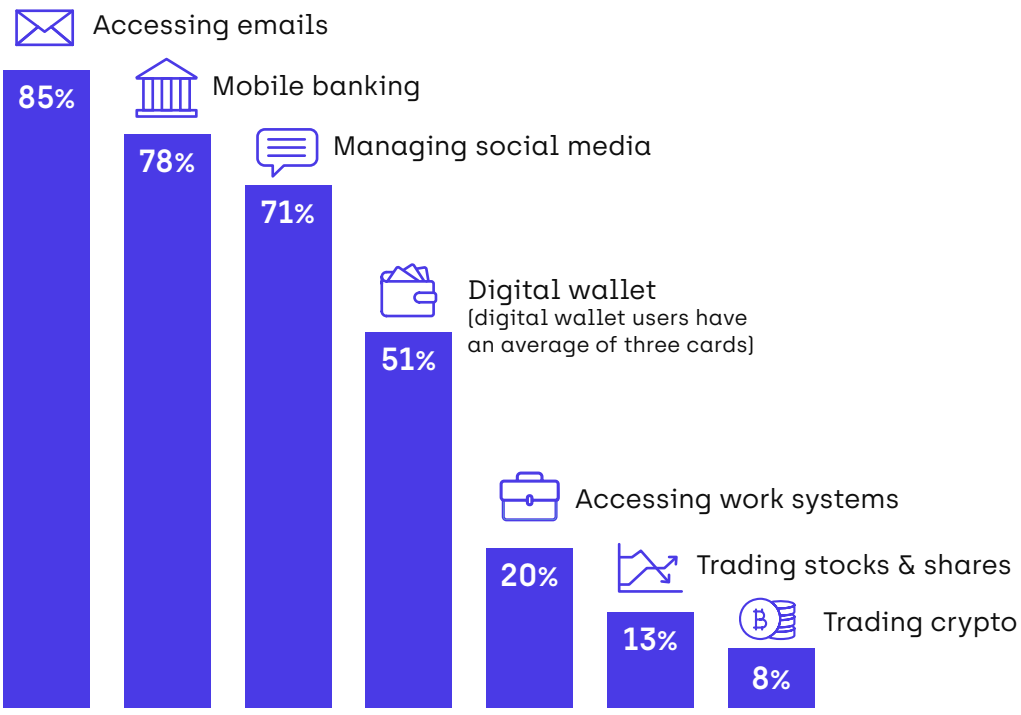
Smartphones: The Gateway To Your Soul?

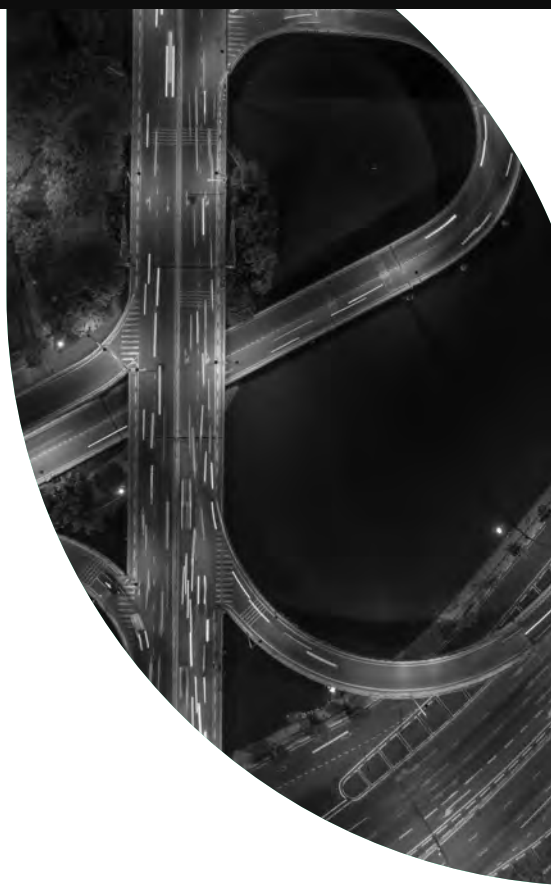
Smartphones now dominate the handset landscape, with UK Smartphone market penetration reaching 90% in 2023. These devices now support a suite of functions, which are embraced by most users.

Nearly four in five (78%) use their smartphone for mobile banking, and over half (51%) utilise digital wallets like Apple Pay and Google Pay. And much like traditional wallets, these digital wallets hold on average three cards, with one in ten digital wallet users having six or more bank cards stored on their device. These figures are significantly higher for those under the age of 45, where two thirds (65%) of users make use of a digital wallet, which indicates that with the passage of time, the overall figure is likely to rise.

Average smartphone usage

How are people using their mobile phone on a daily basis?





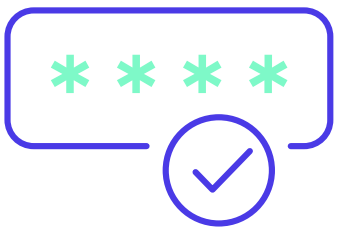
Furthermore, smartphones are used extensively by UK adults to access email (85%), and seven in ten of us use them to manage our social media (71%). Along with the minority of people using their smartphone to manage stocks, shares and cryptocurrencies and work systems like CRM and HR software, this paints a picture of the modern smartphone user.

And this probably goes some way towards explaining why having your smartphone stolen is a concern for 88% of respondents. Your phone has become the de facto means of doing so many things, so much more conveniently. But with all this sensitive information accessible via a single device, there is the potential for significant financial and reputational exposure should it fall into the wrong hands.

PIN-Pointing The Problem

Losing your wallet is a pain. It probably contains all your bank cards, some form of ID, and possibly some cash (although the latter is an increasingly rare feature of the average person's wallet or purse). When you add into the mix all the other capabilities of a smartphone, the risk is elevated. Despite repeated warnings and guidance around password and PIN best practice, nearly half (45%) of smartphone users are in the habit of using the same PIN across multiple apps, services and bank cards. Troublingly, it's the youngest age bracket that demonstrate the worst PIN habits, with the figure climbing to 59%.

We can speculate that this may be because they have less to protect in terms of financial assets, but it is certainly not owing to ignorance. While 50% of over 45s were unaware that you could use the phone's PIN to make payments with your digital wallet, that figure drops to just 20% for for 18 to to 25-year-olds.

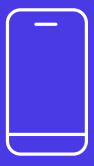


Biometrics were introduced to make smartphones more secure, because the frequency with which you need to input a PIN is greatly reduced, but this has possibly led to some complacency. And it's lead to criminals returning to old school shoulder-surfing tactics to access the phones they then steal. This was a problem highlighted by Detective Superintendent John Roch of the Metropolitan Police in May 2023, who said that though the technology behind apps is secure, criminals are becoming better at exploiting human behaviour.

Various banks and security vendors reacted to the statement by the Met, including Steve Gracey, from HSBC, who said: "There has always been a risk of people being shoulder-surfed when using an ATM, and people are now more conscious of shielding their PIN when withdrawing money. As a result, the way these criminals work means that people should now be more conscious when entering a PIN or a pattern on their phone in a public place, even shielding it like they would when they use an ATM."

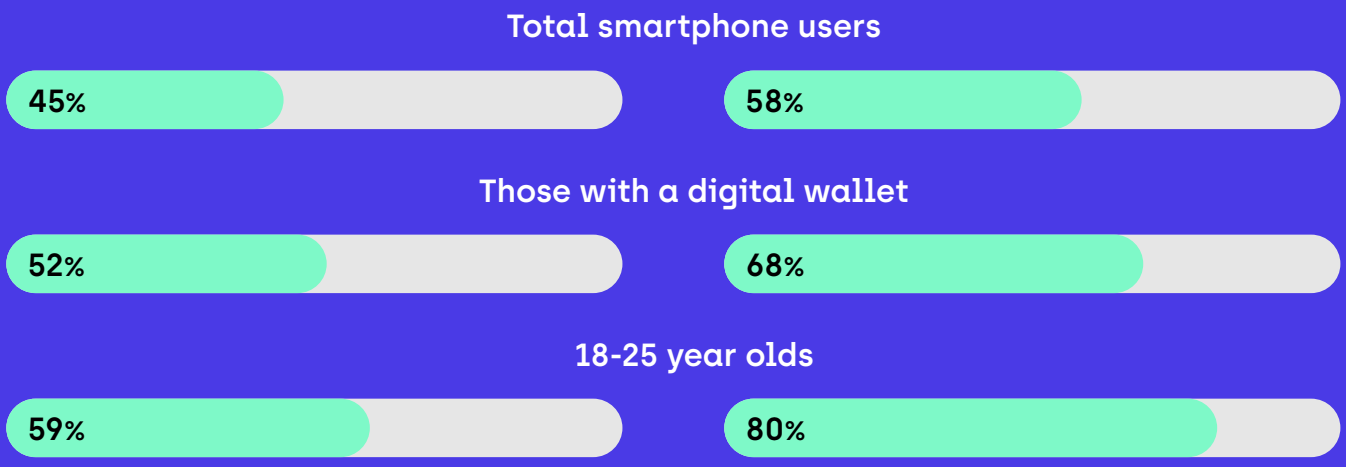
The hidden security risk that having access to a phone's PIN uncovers is the ability to bypass enhanced protections from various providers. Many modern apps and websites require more than just a username and password in the form of a two-factor authentication (2FA) code or a One-Time Password (OTP) from a text message. These measures, which are highly effective against account breaches of laptops offer zero protection when the 2FA code or OTP can be found / received on the compromised device. So how big a problem is this? We decided to find out.

Smartphone PIN security and usage



% who *'always/mostly/sometimes'* have the same PIN for apps on their phone as their phone PIN:

% of those who are aware that bank cards stored in your phone wallet can be used with your smartphone PIN:



Criminal Behaviour

Sadly, the problem is significant. Seventeen per cent of users have had their smartphone stolen, and that figure rises in cities and amongst younger generations. But the loss of the device itself is just the tip of the iceberg and a staggering 62% of respondents who have had their smartphone stolen have suffered further consequences when their device has been accessed. Many had either their social media or emails compromised (which you are usually just logged into on your phone).

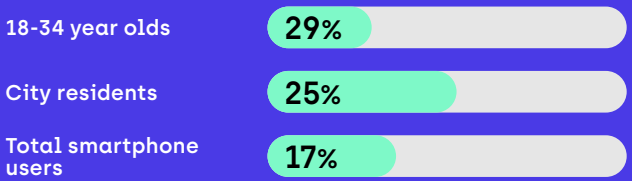
But more worryingly, one in four had money stolen via digital wallets, with one in five having their bank account accessed. While banking apps don't always grant access via your phone PIN, the frequency with which they are broken into, suggests that poor PIN behaviours are hurting people. If smartphone users weren't aware of the risks associated with keeping so much personal information on a single device, those stealing the phones certainly know how to take advantage.

The simplest solution is that we shouldn't be inputting PIN numbers in public, but it's not always that simple or possible, even with the prevalence of face and fingerprint ID systems to access a device, which themselves are not bulletproof. Even if brute force attacks to solve PIN numbers weren't a factor, (and earlier this year, researchers were able to brute force a phone's PIN using a Digispark board, a small ATtiny85-based board with built-in USB connector, and an adapter), biometrics aren't always as secure as you'd hope. Consumer group Which? found that the native facial recognition scanners from several leading manufacturers are vulnerable to spoofing using 2D images. And that's before we consider the potential for generative AI (Artificial Intelligence) to create synthetic biometrics.

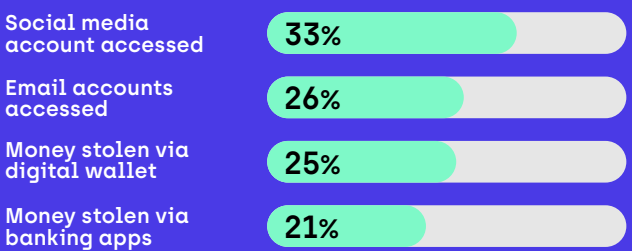
Knowing that this is the next big challenge for security experts to tackle, we asked consumers about their feelings towards AI and whether they believed it increased the likelihood or made it more difficult for someone to gain access to their phone. They're more worried about criminals than they are assured cyber security experts will be able to get the best (or worst) out of AI.

Mobile phone theft

% who have had phone stolen...



What happened when their phone was stolen...



Fixing The Problem

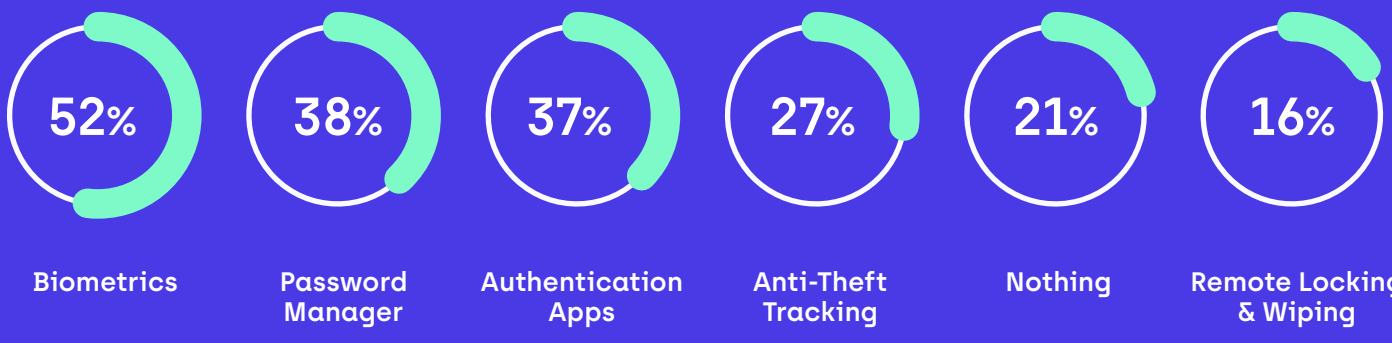
Based on the level and type of smartphone usage, alongside the risk and potential damage of having the phone stolen, device security requires significant improvement and development. Firstly, the risk can be reduced by the individual, through mixing up passwords and PINs, but this is something we've all been told to do before. There are only so many codes, numbers and PINs we can remember.

There are also security measures built into our smartphones such as biometrics, or apps such as password managers, anti-theft tracking software and remote device locking. These all, in certain ways, make it trickier for someone to access a smartphone, or for users to limit the number of passwords and PINs they need to remember. But users may not want to, or be able to, have all these security measures in place (with the exception of built in security features, there is usually a cost associated), or they may just want to protect the most important things. And they are not infallible either.

Modern devices have remote locking and wiping features which aim to prevent thieves from being able to access your device and accounts held on it, but if the thief has managed to observe and learn your passcode, these protections are useless. With your password, a thief can quickly and easily remove your ability to remotely lock or wipe your device. It becomes theirs, not yours, in minutes. Meanwhile, the same thing that makes password managers so convenient (all your passwords are easily accessible in one spot) also represents the greatest risk.

Smartphone security measures

Current mobile phone security measures in place on average:

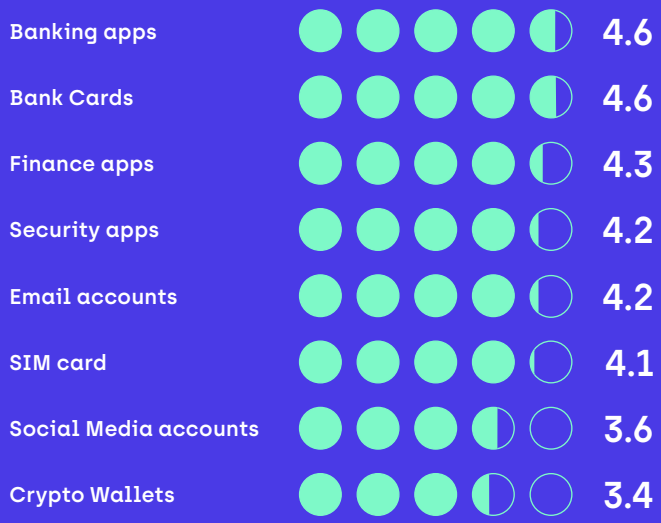


A single point of failure becomes the gateway to an even greater amount of personal information when it is on the device you've had stolen. And what's most important to protect? Whether through bank cards, banking apps or finance apps, the finances accessible through a device is what smartphone users think is most important to protect. This isn't to say someone gaining access to emails or social media can't be extremely damaging, but protecting money is certainly the priority, because the impact is more immediately felt.

Although people feel protecting access to their money is most important, it's probably the area people believe currently has the best, most advanced security measures. The phone PIN is not going anywhere as an essential component of security infrastructure, be that on its own or as part of the known element in a two-factor authentication system. We should be looking to both secure these apps and services that house our personal communication, profile and finances, but also protect them if the worst happens and a smartphone is stolen. It is, therefore, no surprise that three in four showed interest in a service that enables them to cancel cards, block access to bank accounts, email, social media (and more), all in a single activation.

Smartphone security measures

For a service that instantly blocks access to various features, consumers rank (out of five) banking apps and cards as the most important features to protect.



74%

Of smartphone users are interested in a service that allows you to block access to all service simultaneously after the theft of your device.

Conclusion

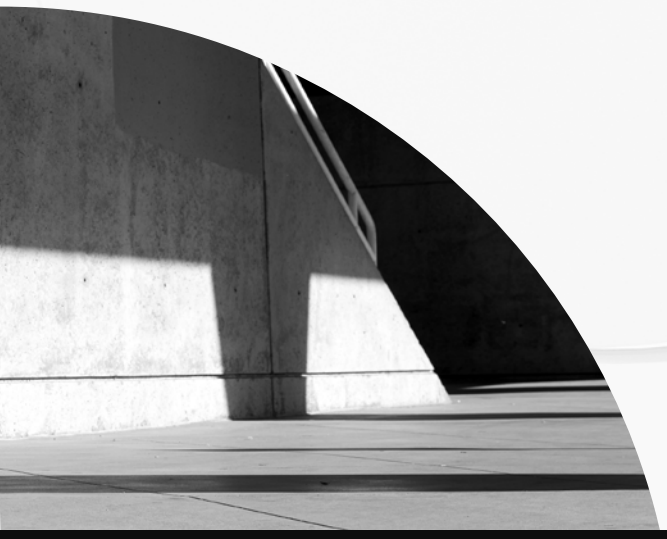
The key takeaway from this research for me is that, given how important phones are in our lives across a breadth of purposes, such as socialising, working and managing our finances, the security and protection we give it, is not appropriately matched. One simple 4- or 6-digit phone PIN that we enter regularly in our daily lives can be used to gain access and control to all of it. It is concerning how low the awareness of this is, particularly amongst those who use digital wallet services.

Given the research quantifies the substantial risk to anyone with a smartphone, it becomes less surprising that of those who had a phone stolen in the past, more were compromised than those who were not. There are plenty of security measures out there, but all have their pitfalls.

Many security measures are preventative, which alongside good user behaviours, decreases the dangers and is, of course, encouraged. However, when reactive measures such as tracking and remote locking software can be disabled after the theft, there is a vulnerability gap that requires additional protection.

For all the reasons addressed in the report, it is no surprise that three in four smartphone users are interested in a service that blocks access to all services simultaneously after theft. I would speculate that if a service such as this was easy to access with a low (or no) cost associated, the uptake would be even higher. Scams, theft, and cybercrime are unfortunately part of life now and we need to stay ahead of it, particularly as risks around security will constantly be changing with the evolution of Artificial Intelligence. Any software that helps us confidently use our mobile devices, in the knowledge that if the worst were to happen, we can protect ourselves more easily, is a welcome addition in my eyes.

Laurence Brown
Senior Insight Manager, KAM



Contact Details & References

KAM
hello@kaminsight.com
www.kaminsight.com

References

https://hackaday.com/2023/07/16/brute-forcing-a-mobiles-pin-over-usb-with-a-3-board/

https://www.which.co.uk/news/article/face-recognition-mobile-phones-axNDM2P9VvyO