COVER STORY

FINANCIAL CRIME

Many of us now store key financial and banking data on our mobiles, making them an even more tempting target for crooks. **Claer Barrett** finds out how we can best protect ourselves

What I wish I'd known before my phone was snatched

It took just seconds for a masked man on an e-bike to snatch my smartphone out of my hands as I waited for a bus in central London in morning rush hour.

He silently cruised up on the pavement behind me, swiping my phone in one efficient, well-practised manoeuvre while I was sending a message. I was stunned, rather than hurt — he barely touched me — but my first reaction was one of fear. Had my phone screen been unlocked?

As he zoomed off, I realised chasing him was futile. Instead, I raced home to kill the phone and secure my data remotely before he could change my passwords and steal from me for a second time.

Phone theft is rising at a rapid pace. And organised gangs know that our smartphones have become gateways to our personal financial information.

They will go to incredible lengths to steal phones unlocked, deploying tactics including "shoulder surfing" and even covertly filming targets to obtain passcodes before phones are stolen, knowing this can unlock passwords for apps and other services.

Disabling a phone's location signal and locking us out buys them more time to plunder our digital wallets, financial apps and steal digital assets such as crypto, plus our personal details and photos. Chillingly, these could be used to defraud us in future — or target friends and family.

I lost a phone and several days of my life dealing with the financial fallout. I was lucky not to lose more. But I have gained valuable knowledge about what is fuelling this crime wave and how we can protect ourselves.

Police are dealing with the highest level of "theft from the person" offences recorded in two decades, according to the latest official figures for England and Wales.

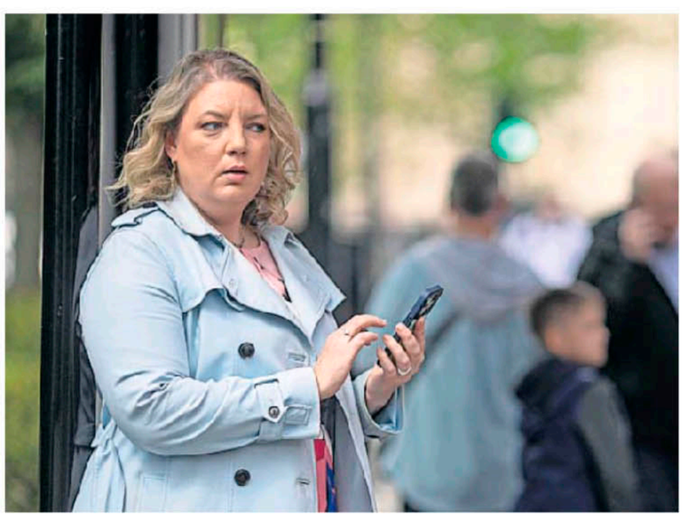
This type of crime — where items are taken without the threat or use of violence — includes pickpocketing as well as snatching. It fell back during Covid, but police records show an 18 per cent increase in the past year; according to Crime Survey data, one in three items stolen is a phone.

London is the epicentre for phone theft. Many people never report this crime, but based on Metropolitan Police data from those who have, a phone is stolen every 10 minutes in the city. There was a 33 per cent increase in reported mobile phone theft from the person in the year to January 2024, and over one-third of offences took place in Westminster.

The statistics don't tell us *how* phones are stolen, but from anecdotal conversations with victims, bike swiping is rife. "Criminals want to make sure when they grab a phone, it's unlocked, otherwise they're going to end up with just a phone," says Tony Sales, a reformed fraudster who founded the crime prevention consultancy We Fight Fraud.

A locked handset could have a street value of a few hundred pounds, he says. But unlocked, it could generate thousands of pounds if criminals can get into the settings, change passwords and compromise other security features.

"It's predatory behaviour," says Sales. "They are like lions stalking prey, and, unfortunately, women make easier targets. It's very unlikely a woman will try to punch you, and a man has more strength to grab someone." The cleaner the snatch, the less likely it is that a screen lock will be activated.



Claer Barrett's mobile phone was snatched as she waited for a bus in central London
Charlie Bibby/FT

It took me 20 minutes to report my phone stolen on the Metropolitan Police website. Four hours later, an email with a crime number informed me they would not be investigating further and my case was closed. But I wanted to know more about what is driving this fast-rising crime.

Sales thinks large increases in the past year have occurred as more gangs realise phone theft is a "lucrative revenue stream". As he says, it requires less effort and violence than drug dealing, with a lower likelihood of getting caught, and lower penalties if you do. The amount of money gangs can make is potentially much higher — especially if they can use your phone to crack your digital life open.

Tech executive James O'Sullivan was drinking with friends in a bar in Dublin last autumn when he realised his phone had been pickpocketed. Assuming face recognition would prevent criminals accessing his device, he thought his biggest problem was not being able to get an Uber home. A day later, he realised he'd lost tens of thousands of pounds.

"I think a spotter observed me using my phone PIN," he says.

Multiple bank and credit cards were stored in his smartphone's digital wallet, and criminals wasted no time purchasing high-value electrical items, spending slightly less than £10,000 on each credit card to avoid triggering daily spending limits.

Marking a phone "lost" by logging into your account online via another device will disable its digital wallet, but O'Sullivan could not do this as criminals had reset his password.

"Crypto and banking apps on your phone are very well protected from someone who hasn't got your phone, but all of the two-factor security codes, notifications and emails to reset passwords are delivered on to the same device," he says.

His banks refunded the stolen money very rapidly, but consumer protections do not extend to stolen crypto, which is much easier for criminals to transfer to their wallet.

Sales agrees crypto apps will be one of the first things a criminal will try to crack, knowing that many users simply store their holdings on an exchange. So-called "cold wallets" — holding assets while unconnected to the internet — are much more secure.

COVER STORY

Dom McKenzie

Transferring money from bank accounts requires a network of money mules to disperse transactions rapidly across multiple accounts. But if criminals have this capability, they will also use people's overdrafts and even apply for personal loans within banking apps, knowing that money can be deposited within minutes.

O'Sullivan has channelled his experiences into launching a new phone security app, Nuke from Orbit. Currently in beta testing, it will act like a digital panic button, allowing users to disable their Sim and an array of online accounts remotely. Tech giants Apple, Google and Samsung are all devising extra security features.

Losses from mobile banking fraud increased by 17 per cent to £18.7mn in the first six months of 2023, the highest recorded total, according to banking trade body UK Finance. The number of cases also hit a new record, increasing by 32 per cent, with average losses per customer of £2,314.

Dianne Doodnath, principal in economic crime at UK Finance, stresses that 98 per cent of unauthorised fraud is refunded within 24 hours of customers reporting it to their bank.

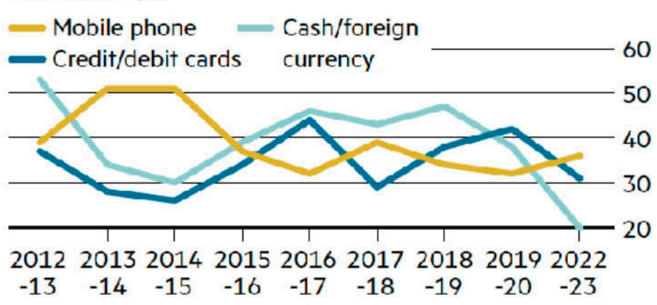
"Millions of people use online banking to transfer money and take out loans legitimately, and we have to strike a balance," she says. "If criminals find more ingenious ways, banks will put more restrictions on."

While consumers want easy access, she says that recently, "some member research is coming back saying people would rather have more friction as it makes them feel safer".

Increasing your own "cyber hygiene" is one way of doing this. Research by Nuke from Orbit found that nearly half of people use the same PIN to gain access to their phone and multiple apps, services, and bank cards, making it even easier for the criminals. Storing multiple bank cards and your driving licence in your phone case is a further gift.

Mobile phones are now more often stolen from people than cash and credit cards

Incidents of theft from the person where each item was taken (%)



No data for the years 2020-21 and 2021-22 due to Covid-19 restrictions
Sources: Crime Survey for England and Wales; ONS

A few days after my phone was taken, I had purchased a new handset and was back up and running on the same mobile number. But my ordeal was not over. Next, the phishing attempts began.

I received a text purporting to be from Apple's "Find My" service saying my lost iPhone had been located, with a clickable link. The FT's cyber security team found this led to a very convincingly designed fake Apple page, asking for my phone's passcode.

I have had phone calls — some automated, some from actual people — claiming to be from organisations I have accounts with, saying they need to "reset my security details". I have not fallen for this. But each time, my heart skips a beat.

Once a criminal gains access to your phone data, there are many other ways they could monetise it. Fraudsters could contact friends or family via social media or messaging apps asking for cash.

If I had nudes on my phone (heaven forfend!) these could have been used to extort money from me.

Challenge a family member to see how far they can get into your phone without your face, but with your passcode. For many apps, if Face ID fails, it defaults to the passcode or a two-factor authentication to reset the password via SMS or email — which of course are delivered to the phone.

As for the phone itself, once the Sim is locked and the phone logged as stolen, it can't be used on any UK networks. However, barred handsets can be shipped overseas and used on foreign networks with a new Sim card.

Met Commander Owain Richards says he understands the impact phone theft can have on victims. "It's an invasive and sometimes violent crime, and we're committed to protecting Londoners and tackling this issue," he says.

Theft hotspots are being targeted with increased patrols and plain clothes officers to deter criminals. "We are also working with phone firms to design out the ability for phones to be reused and sold on," adds Richards.

I now use my smartwatch to tap and pay on public transport and receive notifications from mapping and taxi apps, so my phone can stay zipped up in my bag. I have also reduced the number of cards stored in my digital wallet, and offloaded the bulk of financial apps from my phone to a home-based tablet.

My phone had an array of security features, but sadly, I only found out about some after it was stolen.

Help pages for Apple, Google and Samsung are packed with information about what to do in the event of a theft. Apple's latest iOS update rolled out Stolen Device Protection which helps prevent thieves who know your passcode from making critical changes, such as changing your ID password.

If your iPhone is away from a familiar location such as your home or workplace, a delay of one hour will apply before changes can be made. Plus, biometric authentication will be needed to access stored passwords and credit cards with no passcode fallback. However, you need to activate this and have location services switched on for it to work.

Most Android phones come with a feature allowing you to lock individual apps with a PIN. This creates more friction for criminals — but could also make your phone less easy to use.

You might be able to get a new phone on insurance, restore your data from the cloud and have stolen money refunded. But until this happens to you — and I hope it never does — you simply don't realise how much of your life is on your phone, nor how much hassle and stress its loss causes.

The statistics do not reflect the true cost or seriousness of this crime, nor the level of financial fraud that phone theft enables— or the scale of the black market for stolen devices.

I am holding on to my phone much more tightly these days. Having read this article, I hope you will be too.

Claer Barrett is the FT's consumer editor. claer.barrett@ft.com; Instagram and TikTok @ClaerB