Stolen mobile phone **Shoulder surfing**

Criminals operate everywhere which is why it's important to keep your phone and digital banking details safe. They might try to steal your mobile phone or 'shoulder surf' you.

If your phone has banking apps or saved card details, someone who gets access could attempt to make purchases or send money without your permission.

Shoulder surfing is a social engineering technique where an attacker observes a person's private information, such as passwords or PINs, without their knowledge, often in public settings.

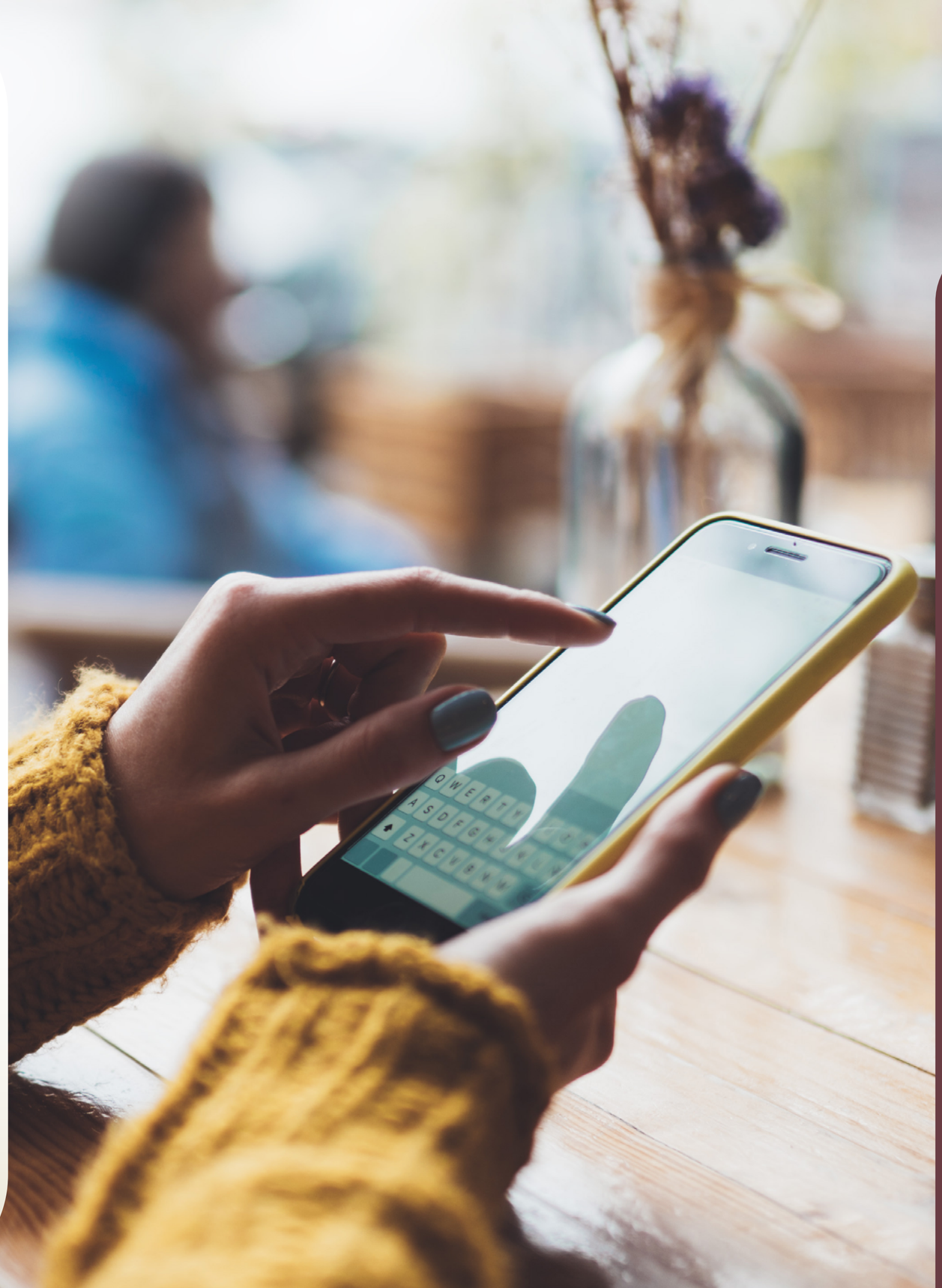
This could take place anywhere – on a bus, at a cash machine, even walking down the street.

Common Scenarios

Shoulder surfing often occurs in crowded places where individuals are less likely to notice someone watching them.

Common scenarios include:

- **ATMs:** An attacker may position themselves behind a user to capture their PIN as they withdraw cash.
- **Public Transport:** Observing someone entering passwords on their mobile device while they are distracted.
- **Cafés and Workspaces:** In open environments, it is easy for someone to glance at another person's screen while they are working or browsing.



How to protect yourself from mobile phone fraud:

- Use biometric data (face or fingerprint) ID if possible.
- Remove banking apps from your phone and keep them on devices that stay at home.
- Use different PIN numbers for unlocking your phone and banking apps.
- Don't store passwords or PINs on your phone.
- Always be aware of your surroundings when accessing financial apps.
- Use Screen Privacy Filters: These filters limit the viewing angle of your screen, making it harder for others to see your information.
- Enable Screen Locking: Always lock your device when not in use and use strong passwords or biometric authentication.
- Check how you can report your phone as lost or stolen on your banking app or website, so you know what to do if this happens.
- Be aware that criminals may try to steal your phone and then pretend they've found it. They might ask you to enter your passcode to prove it's your phone. If this happens, make sure they can't see the passcode as they could try and steal it later.

Scan QR to watch advice from money saving expert Martin Lewis

Courier Fraud

This occurs when a criminal contacts you by phone and convinces you that you are required to hand over money or your debit or credit card for a legitimate reason to someone who will pick this up.

After gaining your trust, the criminals might claim:

- A criminal calls you saying there is a problem with your bank account and gets you to tell them your bank card PIN. They might say there's a fraudulent payment on your card or that someone has been arrested using your details. They then tell you that a courier will pick up your bank card, so that it can be cancelled. With your card and PIN, they can now use your card.
- A criminal may convince you that there is an investigation where they need you to withdraw cash or buy expensive items. This could be foreign or crypto currency, gold bullion, jewellery, mobile phones or designer goods. They tell you this is required so that they can identify the corrupt person. The criminal may pose as a police officer. Once you've bought the items or withdrawn the cash, they'll ask you to give it to a courier, or post it to an address, claiming they'll transfer it to the police. They'll then take the money or goods.
- A fraudster may also say that your bank account has been taken over and that you need to transfer your money to a new 'safe' account. The new account is operated by the criminals, who then steal the funds.
- Some money has been removed from your bank account and that corrupt staff at your local bank branch are responsible. You're advised that someone at the branch has already been arrested but the "police" need you to withdraw your money for evidence.
- That a business, such as a jeweller or currency exchange, is operating fraudulently and they require assistance to help secure evidence.

In these scenarios, the criminals will often tell you not to speak to anyone else about the investigation and promise you will get your money back. They may ask you to lie to your bank or bypass security measures – it is essential that you follow any warnings from your bank and never lie to your bank.

They may offer to send a courier to collect your money, or bank card and PIN. They ask you to write down your PIN and place it in a separate envelope to that of your card.

How to protect yourself

Never hand over your card: Your bank or the police will never ring you to tell you they are coming to your home to pick up money or your card. Never hand these over to anyone who comes to collect it.

Stop and think: Criminals are experts at impersonating banks, trusted organisations or the police. They will try to rush and panic you into responding to their requests. It's ok to reject, refuse or ignore these requests.

Always speak to your bank securely: If you're contacted out of the blue, you can always call your bank back on a number you know to be correct. Hang up and call your bank on a number you know to be true.

Scan QR for more advice our courier scams on the Take Five website