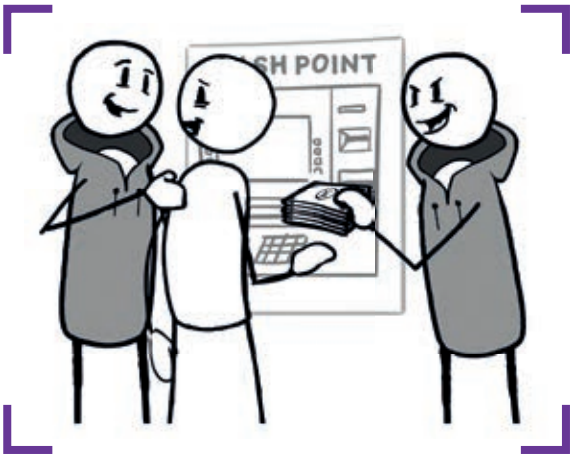
BANKING AND CARD FRAUD – CASH MACHINES

People are targeted at cash machines by criminals who distract users and steal their card or cash. Fraudsters also fit devices to the machines that trap bank cards, copy the card details and record the PIN. You must be vigilant when taking money out of a cash machine and not let anyone distract you.

Criminals may try to see your PIN as you enter it by using a hidden camera or standing nearby. They then attempt to get your card.

They might try and make conversation with you when you are withdrawing money to distract you whilst they or their accomplice takes your card or cash. Criminals have also been known to drop cash on the floor to ask you if it is yours, diverting your attention. They may have fitted a device on the cash machine which either clones your card or retains your card. If your card is trapped in a cash machine by a criminal device, you may leave it unattended to report inside the bank or leave. The criminal will then retrieve the device and your card.

Now the criminal has your card (or a copy) and your PIN.



How to protect yourself

- ⚠ Be wary of anyone approaching you when you are trying to withdraw cash.
- ⚠ Shield your PIN from criminal cameras or prying eyes. Stand close to the cash machine and cover the keypad with your purse, wallet or spare hand.
- ⚠ If there appears to be anything unusual about a cash machine, such as signs of tampering, do not use it and report your concerns.
- ⚠ If your card is retained by a cash machine, report this immediately to your card issuer while still at or near the machine. Store your card issuer's 24-hour contact number in your mobile phone.

BANKING AND CARD FRAUD – CARDS AND CONTACTLESS PAYMENT

Contactless payment is an increasingly popular method of payment, with at least one in three card payments in the UK made using contactless technology. There are many myths that exist relating to the security of this payment system. The information below explains this process, which should ease any concerns you have over this payment method and how it works, whilst giving advice on how to use it safely.

Contactless payment uses a wireless chip containing the user's payment card details which is embedded in a mobile phone or on a bank payment card. This enables users to make payments of up to £30 at stores, cafes and other outlets simply by passing their smartphone or contactless card a few centimetres from a suitable card reader. Some of the security features on this method of payment include the following:

- ⚠ Every contactless card has an in-built security check, which means occasionally you have to enter your PIN number to confirm payment.
- ⚠ Contactless only works when a card or device is within a few centimetres of the reader, making it virtually impossible for details to be intercepted whilst in use.
- ⚠ Whilst a contactless card reader can interrogate a card within 10cm, it will only release the information on the front of the card. For fraud purposes, this is incomplete, and can't even be used to clone the card.

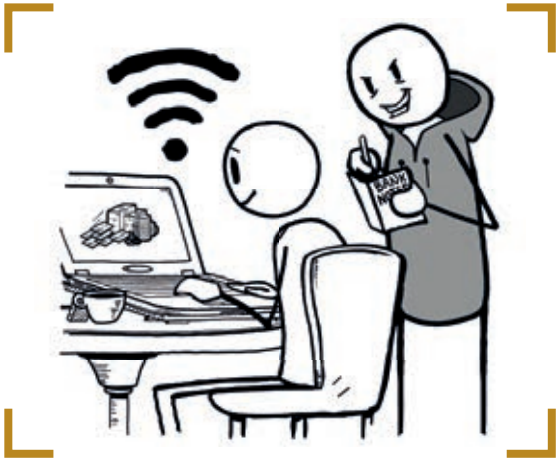
How to protect yourself

- ⚠ Look through all of your bank cards to identify which ones are contactless.
- ⚠ Don't let anyone take your card out of sight while taking a payment – even for just a few seconds. They could be using a skimming device to copy data from your card's magnetic strip, or copying the CCV code on the back.
- ⚠ Monitor your bank statements regularly to ensure that payments have not been taken from your account without your knowledge or permission.
- ⚠ If your contactless payment card or contactless enabled smart phone is lost or stolen, report this to your bank immediately and you should be covered for any subsequent losses.

BANKING AND CARD FRAUD – ONLINE BANKING

The use of online banking or people using banking apps on smartphones and tablets has grown. People use them at home or when they are out and about.

To stay safe while banking online you must protect your password and personal details to stop criminals from accessing your accounts. Many banks provide one-time passcodes sent to your device when setting up new payments. These should never be shared with anyone, even from the bank. If you're speaking to your bank on the phone, and they ask you for it, you are certainly speaking to a criminal, not your bank.



How to protect yourself

- Choose, use and protect passwords and memorable words with great care. Watch the Metropolitan Police's video on passwords at www.met.police.uk/littlemedia for further advice.
- Keep online banking software and banking apps up to date. Always download updates when prompted.
- When logging in whilst in public, take extra care to shield any PIN codes or passwords.
- Always log out of your online banking account or banking app when you have finished using it. Closing the app or web page or turning off your device may not be sufficient.
- Do not use publicly available Wi-Fi networks for banking. It is very difficult to tell if a hotspot is secure.
- Don't share any security codes with anyone.
- If your bank has called you. Take a reference number, and then hang up before recalling on a number you know to be safe after a few minutes to clear the line.