PAYMENT CARD FRAUD

EUROPOL EC3 European Cybercrime Centre

General Advice

Reducing the risk of fraud

With many people becoming a victim of payment card fraud every year, Europol recognises the need to inform the public about basic fraud prevention methods when using a payment card, whether it is a debit, credit, prepaid or any other type of card.

This infographic is intended to prevent payment card fraud from happening to any cardholder, especially during the holiday seasons when people are likely to use their cards in places they are not always familiar with and are therefore more vulnerable to fraud.

Guard your cards and card details

Don't let your card out of sight when making a transaction

Ask the retailer to confirm the amount being debited from your card

Sign new cards as soon as they arrive

Check your receipts against your (online) statements

Carefully discard your receipts from card transactions and information related to your financial affairs

Don't leave your cards unattended in a public place . Keep your personal belongings with you at all times

Never write down your PIN nor disclose it to anyone

When making online transactions, make sure you are using updated antivirus and operating system software

Only buy from trusted sources. For Internet purchases, use the security protocol 3D-Secure

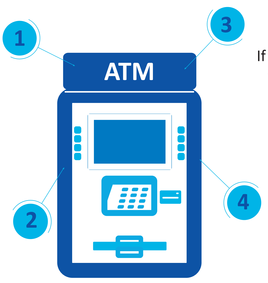
Don't keep your chequebook with your cards

When replacement cards arrive, cut expired/unused/blocked cards into several pieces, including through the magnetic strip and/or chip

Cash Machines (ATMs)

Be aware of others around you
If someone is watching you choose a different ATM

Stand close to the ATM
Always shield the keypad with your spare hand and your body to avoid anyone seeing your PIN



Assess the ATM
If you spot anything unusual about the ATM or there are signs of tampering, don't use the machine and report it to the bank or police

In case of loss
If the ATM doesn't return your card, report it to your bank

Payment Terminals (POS)

Card skimming can occur at retail outlets, particularly bars, restaurants, parking ticket machines and (unmanned) petrol stations

Never lose sight (and, if possible, touch) of your card during payment transactions

Insist that your card is visible to you at all times

Travel - Hotels / Bars / Restaurants

If a hotel stores personal data in your electronic key card, make sure you keep the card with you at all times during your stay and either destroy it afterwards or ensure that the electronic data is erased/wiped/overwritten. Never dispose of used key cards in public bins.

Photocopy of the card
Don't allow the merchant to make a photocopy of the reverse side of your card (the front only is sufficient).

Electronic key cards

ID documents
Don't hand over ID documents (e.g. passport, driver's license) as a 'deposit'. Photocopies are sufficient, and it should be either your ID or credit card details.

PIN
Don't give anyone your PIN number in advance (if you have one) - only when paying the bill.

Your card number and your name should be sufficient to secure payment of the room, facilities & expenses

Card validation
If the merchant swipes your card to validate it, ask what is done with the data, which data is stored, how, where, and for how long.

Card as a deposit
Make sure that your card is returned to you and it isn't kept as a 'deposit'. This isn't safe practice.

What should you do if you become a victim?

Contact your issuing bank or company to cancel the affected card and freeze the associated accounts

If possible, avoid depositing large amounts of money into the affected account

Report the crime to the local police

Monitor your (online) statements and report any suspicious money transfers to your bank

Monitor your credit reports to ensure no-one has opened any new accounts in your name