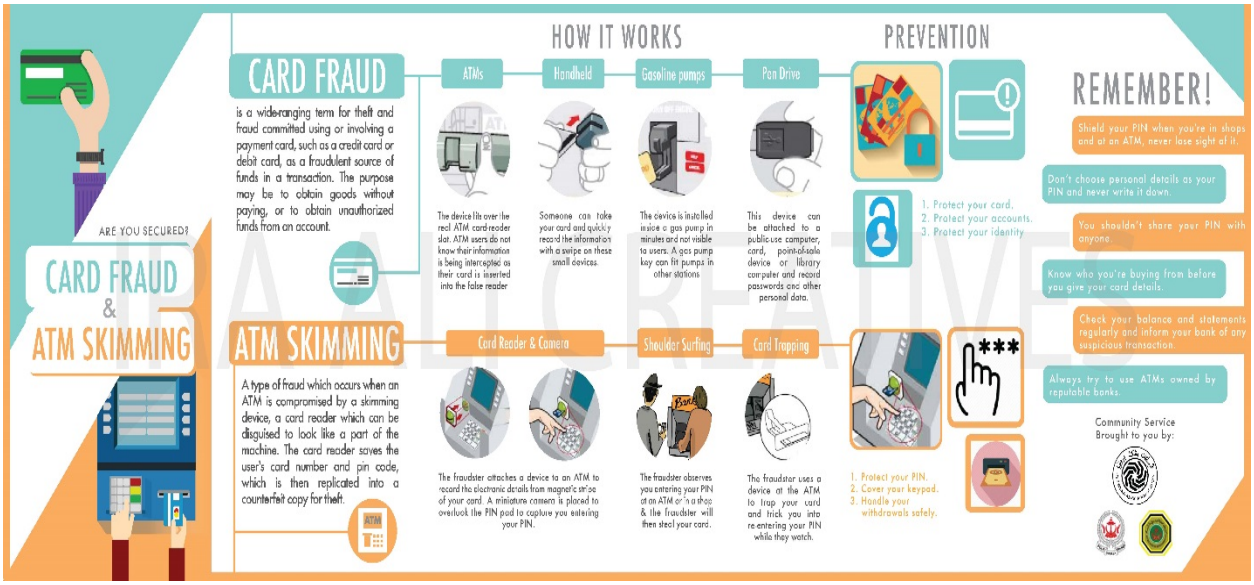
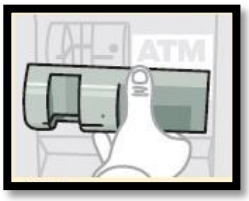
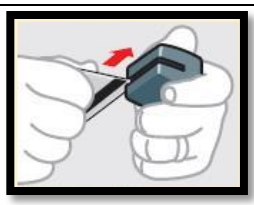
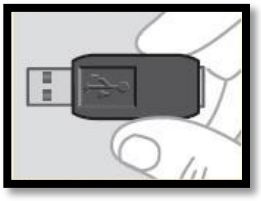


What is Card Fraud and ATM SKIMMING?

Card fraud
is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

How card skimming works
Skimmers are electronic devices used to copy information from the magnetic strips on cards to create 'clone' cards or to make internet purchases. Fraudsters either use or sell the 'clone' cards.

	ATMs The device fits over the real ATM card-reader slot. ATM users do not know their information is being intercepted as their card is inserted into the false reader
	Gas Pump The device is installed inside a gas pump in minutes and not visible to users. A gas-pump key can fit pumps in other stations.
	Handheld Someone can take your card and quickly record the information with a swipe on these small devices.

	Pen Drive This device can be attached to a public-use computer, card point-of-sale device or library computer and record passwords and other personal data.

How to Prevent Card Fraud

Protecting Your Card:-

- Keep your cards in a safe location
- Alert your card company immediately if your card is lost or stolen
- Notify your bank if you will be traveling overseas or far away, or if you are moving
- Keep your eye on your card during transactions

Protecting Your Accounts:-

- Cut up or shred your cards when they expire or you close your account
- Visually inspect ATM machines before using them
- Don't check your finances online while you're in a public place
- Avoid writing down your PIN numbers on or near your cards
- Keep a record of all account numbers in a safe place
- Shred any documents that refer to your account.
- Check your receipts against your statements each month.

Protecting Your Identity:-

- Avoid revealing personal information such as your identity card number or your birthdate unless you initiated the communication.
- Be wary of over-sharing on social networking sites or elsewhere online.
- Shred all documents that contain personal information.
- Report phishing scams immediately to your bank.

ATM Skimming

What is ATM Skimming? Fraudsters place a device on the face of ATM machine and it appears to be part of the machine. Thus, scammers can quickly read a card's information through the device and use it to access your account fraudulently. Your card's information gets stored in the device so that criminals can easily retrieve it later. Alternatively, the criminal will hide a small pinhole camera in a brochure holder near the ATM in order to extract the victim's PIN number.

Fraudsters can attempt to steal cards or card details by using the following methods:

Card Reader & Camera

A fraudster attaches a device to an ATM to record the electronic details from the magnetic stripe of your card. A miniature camera is placed to overlook the PIN pad to capture you entering your PIN. The fraudster can then use the details to produce a fake magnetic stripe card which is then used with your PIN, usually to make ATM withdrawals overseas where Chip and PIN protection is not used.

Shoulder surfing
Shoulder surfing is the term used when the fraudster observes you entering your PIN at an ATM or in a shop. The fraudster will then steal your card by using distraction techniques or pick pocketing.

Card trapping devices
This type of fraud occurs when a fraudster uses a device at the ATM to capture your card. When you use the ATM, your card is retained and the fraudster may trick you into re-entering your PIN while they watch. When your card is not returned, you believe the machine has retained your card and leave to make enquiries. The fraudster then removes the device and your card from the ATM and can use the card to make purchases.

SAFETY TIPS ON USING ATMs

ATM CARDS AND PIN
Keep your Automated Teller Machine (ATM) card safe. Set a PIN that is difficult to guess and different from the ones for other services. Change your PIN regularly. Do not keep your ATM card and PIN together.

ATMs
Beware of anything unusual about the card insertion slot, keypad and keypad cover (e.g. whether any suspicious device is installed). Cover the keypad with your hand when entering your PIN and check whether anyone is trying to peek at your PIN.

HANDLING YOUR CASH WITHDRAWALS
Count the banknotes immediately after each cash withdrawal. Do not take away any banknotes at the cash dispenser or ATM card at the card insertion slot left behind by someone else. Let the banknotes or ATM card return to the ATM automatically.

OVERSEAS CASH WITHDRAWALS
If you intend to withdraw cash from overseas ATMs, check with your bank whether your intended overseas destination can support cash withdrawal using your ATM card. You should also activate the overseas ATM cash withdrawal function in advance and set a prudent overseas ATM cash withdrawal limit and an activation period.

MESSAGES FROM BANKS
Check the transaction records provided by your bank in a timely manner. Inform your bank immediately if you lose your ATM card, or in case of any suspicious transactions or situations. Banks will not ask for any sensitive personal information (including PIN) through phone calls or emails.

DOS & DON'TS

Shops and ATMs
Shield your PIN when you're in shops and at an ATM, never lose sight of it. If an ATM retains your card, report it immediately. Never allow your card to be taken away from you for the retailers to swipe for payments.

PIN and card details
Don't choose personal details as your PIN and never write it down. You shouldn't share your PIN with anyone, not even someone claiming to be from the bank or the police. Use different PINs for different channels (e.g. Internet Banking, ATM and telephone banking) and change them frequently.

Phone and Internet
Know who you're buying from before you give your card details. Never type your PIN into the handset during a phone call. Should you change hand phone number or contact details, to ensure promptly inform your banker. This is to ensure at all times you are informed if any transaction is done.

Keep your bank up to date
Check your balance and statements regularly and tell your bank if you spot anything suspicious. Keep your contact details up to date.

Going abroad
Notify your bank you're going on holiday. Current account and credit card customers can use online travel notification service. Always try to use modern ATMs owned by reputable companies. Avoid stand-alone ATMS. Make sure you have your bank 24hour telephone number for emergencies.

ATM Safety
Don't use an ATM you're suspicious of and never attempt to remove any suspicious device from an ATM. If you're in doubt, inform the bank immediately. Use secured ATM machines – under video surveillance or inside of a bank lobby. They're less likely to be tampered with.

Stranger assistance
Reject any offers of assistance from strangers when you are performing transactions. Don't accept "help" from anybody hanging around the ATM machine. If you encounter any difficulties when using the ATM, cancel your transaction, take back your ATM/credit card and inform the Bank.

Community Service
Brought to you by: