# Payments Security: Safeguarding Your Money

The Payment ecosystem has evolved beyond traditional cash transactions to encompass a diverse array of options, including credit and debit cards, electronic funds transfers, mobile payment apps, online banking, e-commerce, cryptocurrencies, and digital wallets, offering convenience and efficiency, while enabling individuals and businesses to engage in transactions across geographical boundaries and time zones. As reliance on electronic and digital payment services increases, ensuring the security of transactions and preventing fraud become a top priority and of paramount importance for NamPost.

Criminals often target payment systems and payment products due to the inherent financial gains. Fraudsters can exploit weak points in our behavior to steal sensitive financial information or conduct fraudulent transactions. Thus, it is of utmost importance that your personal information is protected.

Below are some specific threats and vulnerability related to ATMs and POS that customers need to protect against.

## ATMs Security Threats and Vulnerabilities

Customers must stay vigilant when using ATMs, as these machines are prime targets for fraudsters There are many ways that fraudsters target ATMs. Common tactics include:

**Cash Trapping:** Fraudsters place a special overlay with adhesive tape on the cash dispensing slot, which blocks the withdrawal of money. In this case, customer may think that the ATM has malfunctioned or has run out of money, the fraudsters to retrieve the money later.

**Skimming:** Fraudsters insert devices to steal and or capture your card information and PIN. This information is then used to siphon money from your account. Fraudsters sometimes set cameras or duplicate keypads on the ATM to record your PIN number and attach a cloning device at the card reading slot.

To mitigate the risks, customers are advised to follow these guidelines when using an ATM:

- Use ATMs located in well-lit and populated areas.
- Avoid ATMs with damaged card slots or keypads.
- Shield the keypad when entering your PIN.
- Collect your card and printed receipts after completing your transaction. Do not leave without it.
- Regularly check your bank statements for any suspicious activities.

Rodney Shivangulula, Head: Payment Solution

## POS Purchase Security Threat and Vulnerabilities

When conducting a transaction at a retail outlet on a point of sale (POS) devices whether it's in a shop or restaurant, be cautious of your surroundings and make sure no one is distracting you or peering over your shoulder to capture your card details. Always follow these essential steps:

- Only use reputable and secure payments outlets.
- Verify the transaction amount before entering your PIN.
- Shield your PIN from prying eyes by using your hand or body to obscure the keypad.
- Be aware of any suspicious attachments to the POS device that could potentially capture your card information.
- Always request and keep your receipt for recordkeeping and protection of sensitive information.
- Regularly check your bank statements for any unusual or unauthorised charges.

Report any suspecious transactions on your Smartcard immediately to your nearest NamPost Post Office or contact the Customer Contact Centre at 061 201 3176.

By following the above precautions, customers can minimise the risks of financial fraud and safeguard your money.

**Financial Services:**
**Tel: 08000 10999 (Toll-free)**
**Email: banking@nampost.com.na**

**www.nampost.com.na**

We Deliver More.

nampost®