PUBLIC NOTICE

Merchant Alert

EFTPOS Skimming

EFTPoS terminal tampering also known as 'skimming', and occurs when someone illegally copies a cardholder's card details to a counterfeit card. If your terminal is not secure, a fraudster could replace your terminal with a tampered device that looks and works like your normal terminal. They could then use the tampered device to steal or copy bank card details to create fake cards and withdraw money from the customer's account.

EFTPoS skimming is difficult to detect and is usually not identified until we find irregular transactions on the cardholder's account.

EFTPoS terminals have many security features which help protect your customers' debit and credit card details. Implementing the below can further protect your business, your reputation and customers against misuse of your terminals and fraud.

You should :

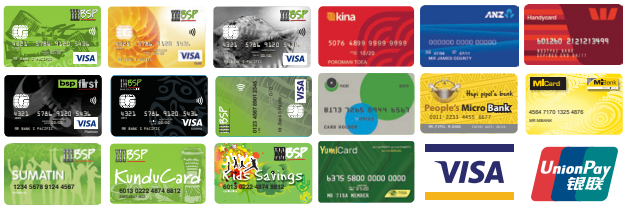
- Keep the terminal in a secure location
- Never leave your terminal unattended
- Create end of day checks to ensure all terminals are accounted for and in working order
- Ensure all employees are fully trained
- Best practice would be to not disclose your terminal password to anyone. However if you need to tell other staff members, make sure you only disclose to a small group of staff to process refunds. They must keep the password a secret

Educate staff to look out for the following irregularities, suspicious behaviours or attachments to a device;

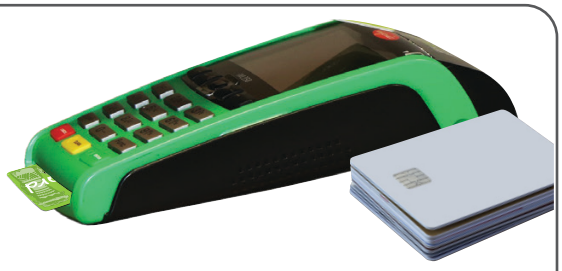
Suspicious | **Safe**

When a card is inserted, it slides further into the device than it normally should. The card should only slide in to read the chip.

We accept



Staff should be aware of the images of cards, pay attention to see if customer is using a card that is blank or unmarked (i.e. blank) or out of the ordinary e.g. a loyalty card or VIP card that is not on card accepted here displays.



Staff should pay attention to abnormal customer behavior;

- Handling multiple cards
- Inputting PIN multiple times

If you believe your terminal, or any other equipment associated with your facility is stolen or tampered with, call us immediately on 3201212/70301212 or email: servicebsp@bsp.com.pg