CENTRAL BANK OF TRINIDAD & TOBAGO

The National Financial Literacy Programme

Be Smart – Save Smart – Live Smart!

CONSUMER PROTECTION TIPS

FOR ELECTRONIC TRANSACTIONS

CONSUMER PROTECTION TIPS FOR ELECTRONIC TRANSACTIONS

TIPS TO PROTECT YOURSELF FROM CARD SKIMMING

Skimming happens when someone uses a card-reading device to copy your account information when you swipe your debit or credit card. In Trinidad and Tobago, card–skimming appears to be most prevalent when bank customers use their bank cards for over–the-counter/point of sale transactions and delivery service transactions.

To prevent against skimming never disclose your PIN (personal identification number) to anyone, and cardholders should be cautious of any suspicious devices involved with an electronic payment. Skimming devices can be installed on an ATM with cameras and overlay touch pads also added to capture your PIN.

- **Never let your card out of sight at the merchant during a payment transaction.**
- **Let the merchant enter the sale amount and, if possible, swipe your card yourself during the transaction.**
- **Cover the keypad of the machine when typing the PIN into the machine.**
- **Record every detail of the transaction, including the date and time.**
- **Take note of the price on the receipt as it may be inflated for incidents of skimming.**

TIPS TO PROTECT YOURSELF FROM PHISHING

Phishing is the fraudulent practice by which a target or targets are contacted by email, telephone or text messaging by disguising oneself as a trustworthy entity to lure individuals into providing personal information, such as passwords and credit card numbers.

One can defend oneself against Phishing or identity theft.

- **Use virus protection software and a firewall on your computer and mobile device.**
- **You can further protect yourself and make sure that your credit card information is sent over a secure server and the information is encrypted with Secure Socket Layer (SSL) technology.**

When an SSL certificate is used the information is protected from hackers and identity thieves. The internet browser will notify you when the server is secure by showing a lock or key icon. In addition, the URL on a secure site is designated by the prefix "https" instead of "http".

DON'T MAKE ONLINE CREDIT CARD PURCHASES FROM PUBLIC PLACES

One should not make online credit card purchases on a public computer. These computers could have keylogger software that will capture all your keystrokes, including your login information and credit card number.

You are not safe just because you are using your own computer or mobile device on a public wifi. Hackers have access to the same Wi-Fi signal and can intercept information while it is being transmitted. Hence you should not conduct online card transactions while using the public Wi-Fi at the airport or a coffee shop.

OUR CONTACT

Tel: 1 (868) 621-CBTT (2288)
or 1 (868) 235-CBTT (2288) Ext 2815-9

nflip-info@central-bank.org.tt

www.nflp.org.tt

@nflptt

The National Financial Literacy Programme@nflptt

The National Financial Literacy Programme (NFLP)
Central Bank of Trinidad and Tobago
Eric Williams Plaza
Independence Square
Port of Spain

CENTRAL BANK OF
TRINIDAD & TOBAGO

Be Smart – Save Smart – Live Smart!