SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

HOW TO PROTECT YOURSELF FROM CARD CLONING OR THEFT VIA THE INTERNET AND CELL PHONES

MOST COMMONLY USED METHODS

PROTECT YOURSELF!

METHODS USED FOR THIS TYPE OF THEFT.

Payment services are increasingly vulnerable to cyber attacks, therefore, the objective is to make known the most common methods used by this type of theft so that users know how to counteract them and avoid being victims of bank card theft.

There are 3 main methods, which are:

1 Card cloning.

An exact copy of the bank cards is created for use to pay in commercial stores or withdraw money at ATMs.

The data is read with a card cloning device called a "skimmer", which is installed in an ATM or store terminal.

Chip cards are not so easy to clone, so cybercriminals infect payment terminals with malicious code that copies user data.

2 Data theft through the Internet.

Fraudsters are looking for bank card details to make online payments which include:

- Card number.

- Expiration dates,

- Verification code (CVV/CVC)

- Name of the card holder,

3 Theft of cards and telephones in an old-fashioned way.

This method of theft is more notorious and blatant, but still common, some of its characteristics are:

1. Cybercriminals use a stolen card to make low-denomination payments which do not require PIN code entry.

2. A phone is always a valuable object for thieves, more so if it has Google Pay enabled, as payments can be made with the phone.

RECOMMENDATIONS.

How to protect yourself from card cloning or theft through the Internet and cell phones.

- ✓ Do not share your password with third parties, make your financial transactions personally.
- ✓ The company and banks NEVER ask you for your financial data or card numbers by phone or internet.
- ✓ Do not give your personal data by e-mail.
- ✓ Carefully review the online payment method and website addresses where you have entered financial information.
- ✓ Set spending limits on everyday cards, if allowed by the bank.
- ✓ Have a virtual card issued with low limits and link it with Google/Apple/Samsung Pay.

TAKE INTO CONSIDERATION...

No establishment should store bank card information.

Bank data theft is doubling every year.

It has been shown that an attacker could also exchange some data with a locked phone and then use modified records from that exchange to make fraudulent payments.

REFERENCES.

Information available on the Internet.

https://latam.kaspersky.com/blog/how-to-protect-emv-and-nfc-bank-cards/26092/