RISKS AND RECOMMENDATIONS
IN THE USE OF AUTOMATIC TELLER MACHINES (ATM)

RISK OF ASSAULT

The probability of becoming a victim of an assault while performing a transaction through ATMs increases if the user:

- Uses ATMs located in unsafe areas,
- Makes his transactions at times of low flow (at night),
- Uses ATMs where there is poor lighting.

To reduce the possibility of being victims of assault, the JEP cooperative recommends:

To use secure ATMs as of the JEP Cooperative, due to its location, lighting, presentation, and availability of the service.

Avoid using ATMs at night or in little-frequented sites.

RISK OF BECOMING A VICTIM OF SOCIAL ENGINEERING

The probability of becoming a victim of social engineering, that is the method by which a unknown confuses the user to obtain the key card or the card of the user through deceptions and win his confidence, increases, if the user:

- Relies on the unknown and gives his key and/or card to this unknown to make the transaction in the ATM.

There are different mechanisms that can be used by criminals once they have deceived their victim. The following is a summary:

Risk of becoming a victim of fraud known as "Switch": Mechanism in which a stranger has earned the trust of the user and obtained the key card (through observation or overconfidence of the user) changes the user card with another person card. Once the key is obtained and the original user card is stolen, the offender comes to withdraw money.

Direct format: Mechanism by which a stranger offers to "clean up" the user card saying there are “reading problems”. The moment in which the user delivers the card to the unknown, he employs a mechanism hidden in his hand that clones information. In order to make the assault, the offender in addition to clone, he must obtain the key card through observation (with a buddy) or through the installation of recording devices superimposed on the ATM.

Indirect format: Mechanism by which criminals mounted false parts that pretend to be authentic with the purpose of obtaining data and key card. The parts are mounted on the original parts of the ATM and these can be

- Fake card readers. They are used to clone the card information.
- Fake keyboards. They are used to record the password entered by the user.
- Fake money dispenser. They are used to retain the money that the user wants to withdraw.
- False upper mount. It is used to hide cameras that record the key entered by the user.

To reduce the possibility of being victims of the cloning of cards, the cooperative JEP recommends:

Note that there is not mounting of parts, presence of adhesives or overlay devices that pretend to be authentic. Note especially: the card reader, the keyboard, and the money dispenser.
DO NOT USE THE ATM to the minor suspicion and immediately report the facts to the institution, owner of the ATM.

Always cover with the other hand when you enter your key..

PHISHING

People close to the environment of the user with easy access to the card and key can take advantage and withdraw money. The probability increases if the user:

- Shares the key with trusted third party
- Has the key written and the third is able to get it. It is common to see that many people have the key written and they take it along with the card.
- Has an easy-to-guess password.

To reduce the possibility of being victims of Pishing, the cooperative JEP recommends:

Change the password of your card periodically if you suspect that it is no longer secret or you used in non-secure ATMs.

MEMORIZE your password. Do not write it anywhere.

Never assign important dates, numbers in sequence, identifying documents, phones numbers, addresses, etc. for your key.

JEP PARTNER ATTENTION SERVICE

If your card has physical wear or malfunction, go to the JEP customer service agencies.

Update your cell phone number to keep you informed about your transactions at ATMs.

In case of loss, theft or if your card has been retained at any ATM, block it immediately.