

Fraudsters arrested in digital payment platforms

Image not found or type unknown



Granma newspaper today published a note explaining the measures taken in response to incidents that occurred last year, where Cuban citizens seized people's email access credentials and committed fraud in the accounts of customers in digital payment platforms through social engineering, traffic capture or Phishing techniques.

Havana, January 31 (RHC)-- Granma newspaper today published a note explaining the measures taken in response to incidents that occurred last year, where Cuban citizens seized people's email access credentials and committed fraud in the accounts of customers in digital payment platforms through social engineering, traffic capture or Phishing techniques.

By the end of December last year, three Cuban citizens living in Havana were arrested. This individuals were engaged in defrauding from their cell phones the accounts of customers who use digital payment platforms, violating the access to the accounts of hundreds of people.

All the accused acknowledged their participation in the facts, the cell phones used to carry out the crime were seized, as well as several magnetic cards, and it has been possible to establish that, from the cell phones of the three accused, they violated the access to the accounts of 351 clients.

It was found that several of those affected filed complaints in 11 provinces of the country, after detecting the extraction of funds from their bank accounts without their consent.

It was also found that, through one of the seized devices, 131 frauds were committed against 68 users between May and October last year, with the amounts stolen exceeding 1,200,000 pesos and more than 7,000 US dollars.

Preliminarily, it was learned that the detainees managed to access the personal data of the victims in records and databases on the Internet, which they compared with those of the digital platforms and, if the possession of an account was positive, they made random attempts to match the payment passwords, many of them too weak, with numbers such as 123456 or dates of birth of the holders.

It was established that the defendants got hold of the victims' email access credentials by means of social engineering, traffic capture or phishing techniques.

According to experts, social engineering is the illicit practice of obtaining confidential information through the manipulation of legitimate users. It is a technique used by cybercriminals to obtain information, access or permissions in computer systems that allow them to harm the compromised person or organization.

Phishing techniques -they point out- is the way in which unscrupulous individuals request information to access any system on the Internet, where they collect personal data from potential victims. In order to stimulate or deceive people to provide their information, they use attractive job offers, promotions, investments, sale of goods, among other tricks, for which they present forms to be filled in by the users.

They also obtain this information from Internet databases that are not protected with security measures and that people, due to ignorance or lack of precaution, think that they will never be used by third parties without their consent.

In another case, operated in April last year in Holguin, the implicated and his wife simulated the interest in acquiring freely convertible currency and, by means of social engineering mechanisms, they requested the information to be used by third parties without their consent, by means of social engineering mechanisms, they requested photos of the cards of presumed clients and the report of the last operations, and with these data they proceeded to steal the available cash.

Part of the criminal activity was generated from publications on the Internet, where the fraudsters promoted the sale of foreign currency at prices below the informal market, through the creation of profiles on social networks with photos and data of previously defrauded victims, this procedure constituting a kind of hook or ruse to attract potential victims.

When contacted by those interested in acquiring foreign currency, the fraudsters identified themselves as trustworthy people, with multiple clients, busy, interested in solving problems with total security and with a strictly legal behavior. Contacts were made via telephone or social networks, never face to face, as well as the method of payment, always by bank transfer.

To try to generate an atmosphere of trust, they were the first to hand over their supposed personal and payment documents (magnetic cards), which, in general, correspond to those of previous victims, or were

obtained by illegal means. To raise the level of trust, they even transfer part of the agreed money.

During 2021, there was an increase in reports of frauds against users who use digital payment platforms, with a predominance of the aforementioned modes of operation, in which the lack of knowledge of the population regarding security and protection of their credentials and passwords is a vulnerability, when the country is advancing in the development of electronic commerce.

In response to these incidents, since last year a group of measures have been adopted to strengthen cybersecurity and customer protection, while reiterating the need to raise the perception of risk with respect to these offenses; refrain from providing personal data to strangers or placing them on social networking platforms that are then used by thieves as a source of information and selection of victims.

It is advisable to systematically check personal accounts; use the double authentication factor, the design and use of strong payment passwords; as well as to pay attention to alerts -via e-mail- on attempts to access their accounts by devices other than those usually used, elements that should be taken into account, because they constitute security mechanisms that shield accounts and prevent access by third parties.

Cuba is committed to developing e-government and e-commerce as a way to meet the needs of the population and the national economy, with particular emphasis on cybersecurity, and will not allow cybercriminals to undermine such strategic purposes for the country, with their illicit activities, which threaten the individual and social heritage of the nation.

<https://www.radiohc.cu/en/noticias/nacionales/284583-fraudsters-arrested-in-digital-payment-platforms>



Radio Habana Cuba