INCREASE IN TELEPHONE SCAMS ASSOCIATED WITH TRANSFERMÓVIL IN CUBA

Press Release No. 46 Food Monitor Program and Cuido60
Havana, 29.04.2026

In recent months, a form of telephone scam has become increasingly established in Cuba in which perpetrators pose as intermediaries of international parcel delivery services. Through calls to landlines or mobile phones, they announce the supposed arrival of shipments—generally medications or food sent from abroad—that must be confirmed through an immediate procedure. During this process, victims are asked to enter codes or make transfers through the Transfermóvil application. Once the operation is completed, the funds are withdrawn and the scammers cut off communication.

The increase in these practices has been noted by banks and payment platforms; however, the scale of the phenomenon continues to grow due to the limited coverage in the official press, the absence of prevention strategies by official civil society bodies, as well as the inaction of authorities responsible for ensuring the implementation of public policies for prevention, investigation, and redress.

Digital crime and multifactorial crisis:
Various international organizations have reported an increase in digital crime associated with periods of economic recession and rising living costs. In Cuba, however, this phenomenon takes on specific features that merit particular attention:

- Increased inequality in access to basic goods and services, particularly food and medications
- Growing population aging and an increase in households without effective support networks
- Recent incorporation of digitalization processes, with limited knowledge and digital literacy regarding risks and scam methods (identity theft, data theft, deception and telephone scams, cyberattacks on accounts, etc.)
- Normalization and expansion of unverifiable informal channels, dependent on intermediaries, for accessing necessary goods
- An inefficient and poorly prepared bureaucratic apparatus that hinders legal actions for investigation and prosecution
- Forced banking digitalization due to cash shortages

Older persons: a highly vulnerable group

Older persons constitute one of the groups most exposed to this type of scam. In Cuba, where demographic aging is among the most advanced in Latin America, one quarter of the population is over 60 and depends on limited pensions, remittances, or family support. This group faces specific conditions that increase its vulnerability: lower digital literacy, reduced

access to up-to-date information on fraud, and, in many cases, a greater predisposition to trust calls appealing to urgent needs such as medications or food.

Digital literacy represents another major challenge, as older persons, being digital migrants, encounter greater difficulties adapting to new technologies. At the same time, the scarcity of programs aimed at improving knowledge and skills in the use of new technologies among this population increases their exposure when using “smart” devices, engaging with virtual payment gateways for many basic services, and interacting on social networks and virtual communities. Through its monitoring work, Cuido60 has documented the existence of a digital divide driven, among other factors, by restrictions in access, information, training, and ageism. The prevalence of negative stereotypes regarding the learning capacities of older persons—especially in technological matters—constitutes an additional barrier that limits access to digital platforms and increases risk in their use.

As a result, FMP and Cuido60 warn about the immediate implications of this phenomenon in a society experiencing reduced access to basic goods and services necessary for a dignified life, limited access to justice, loss of trust in official institutions, delegation of state responsibilities to private individuals, dependence on opaque arrangements for survival, and an increase in crime driven by power vacuums.

Recommendations for the public

Individual prevention, while necessary, does not replace the importance of structural mechanisms for protection, monitoring, and response. However, given the limited availability of information addressing this issue, FMP and Cuido60 recommend that the population adopt the following preventive measures:

1. DO NOT make transfers or confirmations in response to unverified calls or codes, even if presented as official institutions (fraudulent impersonation and identity theft).
2. DO NOT share codes, PINs, or personal data under any circumstances (personal data theft).
3. Be wary of artificial urgency (24–48 hour deadlines, pressure to act immediately).
4. DO NOT return calls to unknown numbers requesting payments or data.
5. Consult family members or trusted third parties before carrying out unusual financial operations.
6. Report suspicious numbers to close contacts and on social media.
7. Keep applications updated and activate available security measures.
8. Report incidents, even if the money is not recovered, to contribute to the visibility of the phenomenon.
9. Participate in digital literacy programs and stay informed about common risks and prevention measures.

Recommendations for the State and civil society organizations

10. Expand digital literacy programs specifically for older persons in collaboration with civil society organizations.
11. Develop awareness and information campaigns to support older persons in the use and management of virtual platforms and payment gateways, as well as to prevent cybercrime.
12. Support community programs that promote accompaniment of older persons in learning new technologies and digital rights.
13. Define the institutional framework responsible for public policy in this area, particularly regarding older persons.
14. Improve the handling and processing of cybercrime complaints from older populations.

15. Equip the judicial system with tools and capacities to process this type of crime.
16. Review and adjust existing regulations on cybercrime.
17. Train human resources within police forces and the judicial system to respond to the growing demands related to cybercrime.