AUMENTO DE ESTAFAS TELEFÓNICAS ASOCIADAS A TRANSFERMÓVIL EN CUBA

Nota de prensa No. 46-Food Monitor Program y Cuido60

La Habana, 29 de abril de 2026

En los últimos meses se ha consolidado en Cuba una modalidad de estafa telefónica en la que los perpetradores se hacen pasar por intermediarios de servicios de paquetería internacional. A través de llamadas a líneas fijas o móviles, anuncian la supuesta llegada de envíos –generalmente de medicamentos o alimentos remitidos desde el exterior– que deben ser confirmados mediante un procedimiento inmediato. Durante este proceso, solicitan a las víctimas introducir códigos o realizar transferencias a través de la aplicación Transfermóvil. Una vez realizada la operación, los fondos son sustraídos y los estafadores interrumpen la comunicación.

El aumento de estas prácticas ha sido advertido por bancos y plataformas de pago, sin embargo, la magnitud del fenómeno continúa aumentando ante la escasa cobertura de la prensa oficial, la ausencia de estrategias de prevención por parte de órganos de la sociedad civil oficial, así como por la inacción de las autoridades que deberían velar por la ejecución de políticas públicas de prevención, pesquisa y reparación de daños.

Crimen digital y crisis multifactorial:

Diversas organizaciones internacionales han reportado un incremento de crímenes digitales asociado a periodos de recesión económica y al aumento del costo de vida. Sin embargo, en Cuba este fenómeno cobra sus propias particularidades dignas de subrayar:

- Aumento de desigualdad en el acceso a productos y servicios básicos, principalmente alimentos y medicamentos
- Aumento de envejecimiento poblacional y de hogares sin redes de apoyo efectivas
- Reciente incorporación de procesos de digitalización, limitados conocimientos y alfabetización digital sobre riesgos y métodos de estafas (suplantación de identidad, robo de datos, engaños y estafas telefónicas, ciberataques a cuentas, etc.)
- Naturalización y ampliación de vías informales no verificables, dependientes de intermediarios, para el acceso a productos necesarios
- Ineficiente y poco preparado aparato burocrático que obstaculiza acciones legales para la pesquisa y penalización del delito
- Forzada digitalización bancaria ante escasez de efectivo

Personas mayores: grupo de alta vulnerabilidad

Las personas mayores constituyen uno de los grupos más expuestos a este tipo de estafas. En Cuba, donde el envejecimiento demográfico es uno de los más avanzados de América Latina, un

cuarto de la población supera los 60 años y depende de pensiones limitadas, remesas o apoyos familiares. Este grupo enfrenta condiciones específicas que aumentan su vulnerabilidad: menor alfabetización digital, menor acceso a información actualizada sobre fraudes y, en muchos casos, una mayor predisposición a confiar en llamadas que apelan a necesidades urgentes como medicamentos o alimentos.

La alfabetización digital es otro de los grandes desafíos, ya que las personas mayores, al ser migrantes digitales, encuentran más dificultades para adaptarse a las nuevas tecnologías. Al mismo tiempo, la escasez de programas orientados a mejorar los conocimientos y destrezas en el uso de las nuevas tecnologías en este grupo poblacional, aumenta la desprotección frente al uso de dispositivos "inteligentes", la introducción de pasarelas virtuales de pago de muchos servicios básicos, así como la interacción en redes sociales y comunidades virtuales. En su labor de monitoreo, Cuido60 ha documentado la existencia de una brecha digital provocada, entre otros aspectos, por restricciones de acceso, información, capacitación y edadismo. La prevalencia de estereotipos negativos respecto de las capacidades de aprendizaje de las personas mayores, especialmente en relación con temáticas de orden tecnológico, es una barrera adicional que dificulta el acceso a las plataformas digitales y aumenta el riesgo en su uso.

En consecuencia, FMP y Cuido60 alertan sobre las implicaciones inmediatas de este fenómeno en una sociedad que reporta pérdida de acceso a productos y servicios básicos para sostener una vida digna, limitado acceso a la justicia, pérdida de confianza en las instituciones oficiales, responsabilidad estatal delegada sobre personas privadas, dependencia de contratos opacos para sobrevivir, aumento de la criminalidad motivada por vacíos de poder.

Recomendaciones para la ciudadanía

La prevención individual, aunque necesaria, no sustituye la importancia de mecanismos estructurales de protección, monitoreo y respuesta. Sin embargo, ante la escasa información de vías abordando este problema, FMP y Cuido60 recomiendan a la población adoptar las siguientes medidas de prevención:

1. **NO realizar transferencias ni confirmaciones** ante llamadas o códigos no verificables, incluso si se presentan como instituciones oficiales (personificación fraudulenta y robo de identidad).
2. **NO compartir códigos, PIN ni datos personales** bajo ninguna circunstancia (robo de datos personales).
3. **Desconfiar de urgencias artificiales** (plazos de 24–48 horas, presión para actuar de inmediato).
4. **NO devolver llamadas** a números desconocidos que soliciten pagos o datos.
5. **Consultar con familiares o terceros de confianza** antes de ejecutar operaciones financieras no habituales.
6. **Reportar números sospechosos** a contactos cercanos y redes sociales.
7. **Mantener actualizadas las aplicaciones** y activar medidas de seguridad disponibles.
8. **Denunciar los hechos**, aun cuando no se recupere el dinero, para contribuir a la visibilización del fenómeno.
9. **Participar de programas de alfabetización digital** e informarse de los riesgos más comunes y las medidas de prevención.

Recomendaciones para el Estado y las organizaciones de la sociedad civil

10. **Ampliar programas de alfabetización digital** específicos para personas mayores en colaboración con organizaciones de la sociedad civil.
11. **Desarrollar campañas de sensibilización e información** que ayuden a las personas mayores en el uso y manejo de las distintas plataformas virtuales y pasarelas de pago, así como a prevenir los ciberdelitos.
12. **Apoyar programas comunitarios** que fomenten el acompañamiento a personas mayores en el proceso de aprendizaje de las nuevas tecnologías y de los derechos digitales.
13. **Definir la institucionalidad** que se ocupará de la política pública en la materia, en particular, en lo referido a las personas mayores.
14. **Mejorar la atención y tramitación de denuncias de ciberdelitos** de la población mayor.
15. **Dotar al sistema judicial de herramientas y capacidades** para procesar este tipo de delitos.
16. **Revisar y ajustar la normativa existente** en materia de ciberdelitos
17. **Capacitar a los recursos humanos** de los cuerpos policiales y del sistema judicial para las nuevas demand as en relación con el aumento de delitos cibernéticos.