# Tips para cuidar el dinero en las billeteras digitales


Las billeteras digitales se han convertido en una herramienta que entrega mucha facilidad a los usuarios para mover su dinero, permitiéndoles hacer transacciones de grandes cantidades hasta pagos en las tiendas en los barrios. Pero también son un reto para la ciberseguridad, porque los delincuentes se fijan en ese crecimiento y van tras el dinero.

Durante el 2021 las fintech en Latinoamérica aumentaron a casi 2.482, de esas aproximadamente en **Colombia** hay 279, en **México** al 512 y en **Brasil** hay 771. Dentro de las que se destacan plataformas como las billeteras y las bancas móviles que permiten pagos sencillos y desde el celular.

Además, solo en Colombia, entre el primer semestre de 2021 y el mismo periodo de 2022 se incrementaron en un 47,6% las transacciones digitales. Tiempo en el que se detectaron cerca de 9 mil millones de intentos de robo en estas plataformas, por lo que los usuarios deben saber cuidar su datos y dinero.

# Cómo cuidar la seguridad de una billetera móvil

El primer punto a tener en cuenta es que estas aplicaciones están diseñadas en gran porcentaje para celulares, así que el primer cuidado siempre debe ser proteger el teléfono de cualquier vulnerabilidad. Para eso es clave no instalar softwares peligrosos, de procedencias extrañas y mantenerlo instalado.


Este tipo de aplicaciones se deben cuidar como los procesos bancarios para no perder el dinero.

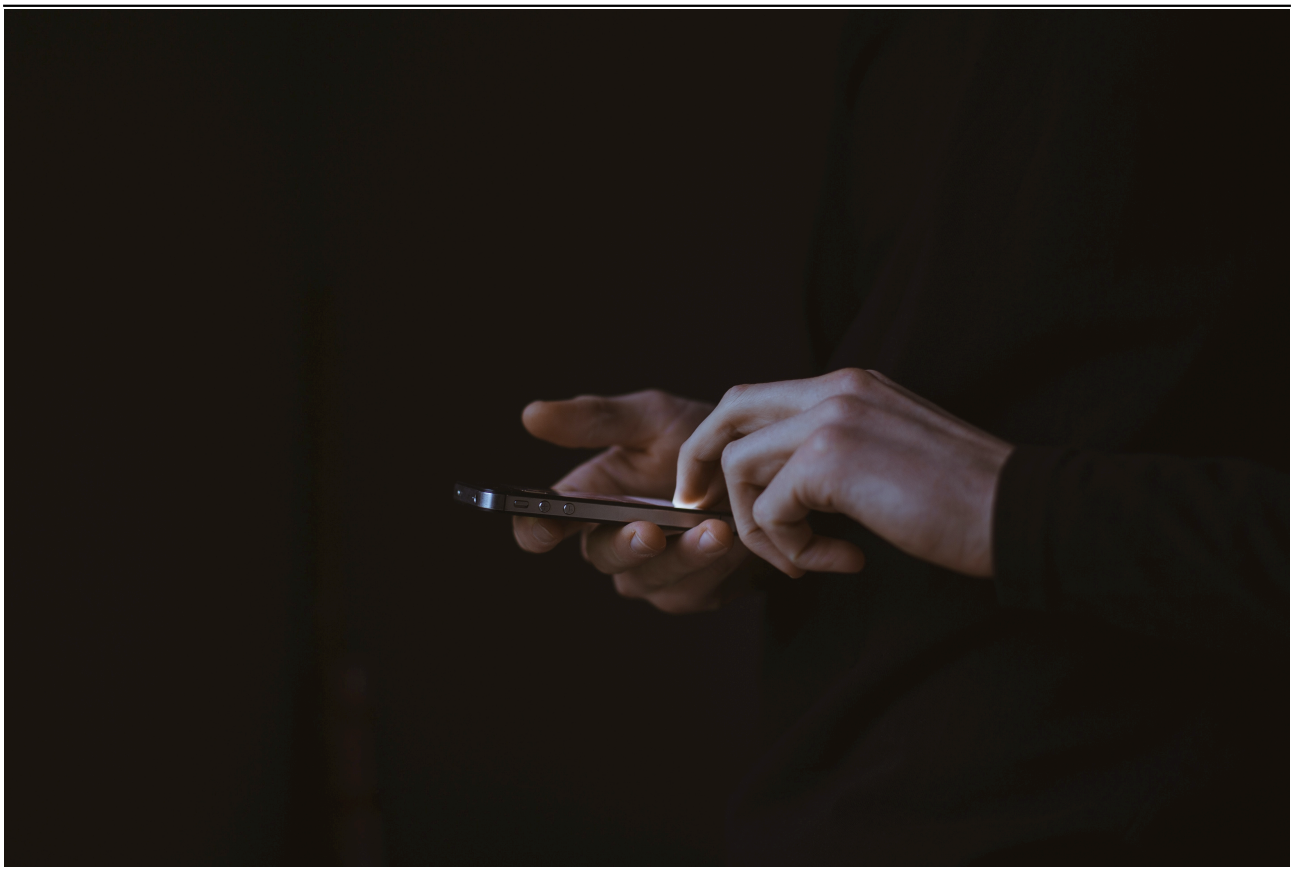
“Un sistema operativo seguro se puede volver inseguro haciendo eso, ya que puede recibir actualizaciones de otras fuentes en donde no se sabe qué problemas pueden generar y pueden instalar aplicaciones que no han sido validadas por Google”, afirmó Ricardo **Villadiego**, CEO de **Lumu Technologies**, empresa especializada en la seguridad de estas plataformas.

Otro paso importante es pensar que la aplicación es una extensión del banco y de esa forma tener los mismos cuidados que tradicionalmente se han mantenido para esos procesos físicos, como no compartir contraseñas, modificarlas cada cierto tiempo, tener un acompañamiento en caso de no entender su funcionamiento, verificar datos, entre otros.

“El usuario tiene que tener las mismas prácticas que utilizan cuando interactúa con su banco, asegurar que no está recibiendo mensajes de texto de que no vienen del proveedor de la billetera móvil, además de correos que suplantan a la billetera móvil con el objetivo de robarle sus contraseñas y posteriormente tener acceso”, afirmó.

Pero en medio de todo este panorama hay situaciones que para un usuario común es difícil controlar, como la reciente modalidad de clonado de SIM con la que los delincuentes suplantan el número de teléfono y de esa forma obtienen códigos de acceso o segundas claves de las cuentas.

Por eso la recomendación de los expertos es que en caso de perder un celular o de ver que están expuestos a una situación así, lo primero que se haga es bloquear todos los servicios financieros antes que el propio teléfono, porque va ser tiempo que se le está “regalando al cibercriminal para realizar transacciones”.



Lo delincuentes también avanzan con facilidad para crear nuevos métodos de robo en aplicaciones.

Finalmente, **Villadiego** pone un ejemplo de cómo la seguridad física debe replicarse en la digital: pensar antes de dar clic.

“Tenemos que pensar en esa cultura del mundo físico cuando yo voy a cruzar la calle: paro y miro a la izquierda y a la derecha para validar qué puedo cruzar. Seguramente eso en el mundo físico es fácil de detectar, porque en el mundo cibernético no es tan sencillo, pero cada vez que voy a dar clic hay que pensar antes si puede ser un problema o no”.

Esto último muy relacionado con los mensajes o las cadenas en redes sociales que invitan a las personas a entrar a un enlace prometiendo algún dinero, trabajo, información y demás, pero que en realidad son páginas falsas que roban datos o instalan malware.

## No tener miedo a usarlas

Si bien nunca un sistema va a ser 100% seguro, para **Villadiego** las transacciones en línea y por billeteras digitales son mucho más seguras que ir al banco de forma tradicional, porque el número de problemas de seguridad es “ínfimo, comparado con el número de operaciones exitosas”.

Como ejemplo, pone que su empresa entre el primer semestre de 2021 y el primero de este año bloqueó exitosamente 9 mil millones de intentos de robo.

Aunque hace un llamado a todas las entidades involucradas, especialmente los bancos, a que nunca bajen la guardia, porque el crecimiento tecnológico también trae avance en los ciberdelincuentes y la fórmula nunca es exacta.

“El adversario va a seguir evolucionando, no hay un control de ciberseguridad que te va a proteger hoy y hacia el futuro. Por lo que las compañías tenemos que seguir evolucionado de la misma manera y la mentalidad de control, por no significa que lo que hoy es efectivo asía va a ser el resto de la vida”, concluyó.