DIALOGUEMOS
La academia en la comunidad



Wilson Araque | Universidad Andina Simón Bolívar | lunes, marzo 4, 2024

Es responsabilidad prioritaria de los servicios financieros garantizar la seguridad de las transacciones. Los usuarios deben poder alertar y bloquear tarjetas rápidamente y, así, parar, al instante, el proceso fraudulento que está ocurriendo debido a la presencia de ciberdelincuentes

Tiempo de lectura: 3 minutos

En primer lugar, es responsabilidad prioritaria de los oferentes de servicios financieros garantizar la seguridad continua de las transacciones relacionadas a los productos que ofrecen; siendo para ello necesario que, como punto clave, faciliten de forma amigable y, a tiempo, los reclamos, sobre todo, cuando los usuarios buscan alertar y/o pedir el bloqueo de instrumentos como, por ejemplo, las tarjetas de crédito y, así, parar, al instante, el proceso fraudulento que está ocurriendo debido a la presencia de ciberdelincuentes que, ahora con la aceleración de la digitalización, son los que más han crecido en número y en sus capacidades de “creatividad al servicio del mal”.

Los organismos de control como la Superintendencia de Bancos (SB) y la de Economía Popular y Solidaria (SEPS) son, también, otro de los actores que tiene una gran responsabilidad para fortalecer la seguridad al momento que ocurren transacciones financieras. Por ejemplo, es clave que se obligue -sin excepción- a todo negocio -que, como parte de sus medios de cobro, tiene el servicio de tarjetas de crédito- a que el registro de datos de la transacción se realice a la vista del cliente propietario de la tarjeta y, así, evitar malas prácticas de robos de datos que, cuando las transacciones, luego, se hacen sin la tarjeta física, tienden a ser usados y, mediante ese mecanismo delincuencial, dar inicio a graves estafas.

De ahí, la seguridad en las transacciones financieras debe tener un enfoque“de total” considerando diferentes puntos de responsabilidad iniciando, como es obvio, con el propio usuario del producto financiero -tarjetas de débito y crédito, cheques, claves digitales, etc.-; luego con quien es el emisor

financiero y, por supuesto, también de quienes son las empresas oferentes de los bienes y/o servicios que son objeto de la transacción. Más, como ya se resaltó, cruzando transversalmente -a todos los responsables anteriores-, el rol de vigilancia de los organismos de control respectivos.

En el caso del usuario, este debe ser cuidadoso de sus claves que, para operaciones físicas y/o digitales, son las que autorizan se realice determinada operación. Para ello, hay que crear claves con signos difíciles de copiar, luego guardarlas en lugares seguros, no compartiendo a terceros y, regularmente, irlas cambiando. También, es importante que se esté pendiente de los mensajes de texto digital y/o de correo electrónico en donde, generalmente, se alerta de compras que, si la persona no hizo, se convierte en el inicio de un largo problema potenciado por la estafa financiera que se está sufriendo; ya que, ahora, los delincuentes como saben que las personas poco revisan esos medios de comunicación digital -por su concentración casi total en los servicios de redes sociales virtuales-, simplemente, aprovechan de ese escenario para hacer de las suyas hasta cuando llega el estado de cuenta mensual y, recién ahí, el usuario identifica las sorpresas de consumos no realizados.

Otra recomendación clave, es tener a la mano los medios de contacto para hacer el bloqueo inmediato cuando, sorpresivamente, asoman aquellos consumos no realizados por el tarjetahabiente titular. Y lo otro, también, clave es exigir que, delante de cada usuario, se proceda a pasar, por ejemplo, la tarjeta, en el instrumento facilitador de la transacción y, así, evitar clonaciones basadas en la toma de fotografías de las tarjetaspara apropiarse de los datos que, luego, les ayudan a los ciberladrones a realizar sus fechorías.

Completando las recomendaciones desde la responsabilidad del propio usuario y pensando en una “seguridad financiera 360”, es recomendable, también, que quien tiende a usar productos financieros digitales acuda, solamente, a aquellos lugares comerciales confiables que, con evidencias, demuestren tener existencia formal.

Finalmente, desde el lado de las entidades emisoras, también es fundamental su accionar; pues, si le va mal al usuario con el producto financiero entregado, simplemente, dejará de usarlo y, además -como peor escenario-, por la insatisfacción generada se encargará de difundir su malestar enfatizando, sobre todo, en el peligro que significa usar el producto financiero de determinado emisor.

Surgiendo, así, una necesidad que además de brindar todas las seguridades informáticas y de procedimientos operativos a los usuarios, también, por un lado, se oriente a su capacitación en ciberseguridady, por otro, se enfoque a la buena y confiable selección que se haga de los comercios con quienes el cliente financiero va a interactuar al producirse cualquier tipo de transacción financiera; evitando, de esa forma, que inescrupulosos usen el escudo de un producto financiero -otorgado, sin las medidas preventivas respectivas, por parte de un determinado emisor formal- para realizar transacciones de dudosa ejecución y, con ello, afectar negativamente al patrimonio de miles de usuarios.