

Por qué es segura la banca electrónica

En los tiempos que corren, nadie se atreve a aponer en duda que nuestra vida diaria se ha sumido en un sinfín de operaciones tecnológicas. Podemos decir que, para la mayoría de nosotros, el mundo se ha digitalizado a un extremo que hasta hace poco era difícil de predecir. Hablar por teléfono, leer, escuchar música, estudiar o ver las fotos de nuestros familiares y amigos, son hoy tareas enteramente digitales.

Nos hemos acostumbrado a la tecnología y hemos aprendido a confiar en ella, y esto incluye el campo de las finanzas personales. Nuestras consultas y operaciones bancarias han ido trasladándose a la banca electrónica y a Internet, y los instrumentos financieros del “antiguo” mundo analógico, como el dinero en efectivo y los vetustos cheques, van perdiendo terreno rápidamente.

A pesar de ello, aún encuentro gente que mantiene dudas, siempre razonables, acerca de la seguridad de las transacciones electrónicas en comparación con las que solíamos hacer en las taquillas de los bancos, siempre con soportes físicos en papel. De vez en cuando leemos en los periódicos llamativos titulares sobre el descubrimiento de redes de estafadores que intentaban hacerse de grandes fortunas mediante fraudes computarizados, o aventureros “hackers” descubiertos después de violar intrincados mecanismos de seguridad electrónica. Todo esto, por supuesto, lleva al público a preguntarse de nuevo qué tan seguro es este mundo de las finanzas electrónicas.

Pues bien, la realidad es que, después de apartar esos casos puntuales que en contadas ocasiones ocurren -y que casi siempre conocemos después de que las autoridades atrapan a los estafadores informáticos- las operaciones de comercio y de banca electrónica, y la propia Internet, son cada vez

más seguras: Los sistemas que respaldan las transacciones bancarias son más robustos y están en permanente mejoramiento. Lo cierto es que estas operaciones, aunque no sean infalibles, son mucho más seguras que las que se hacen en cheque. Y ni hablar del efectivo.

Si no lo cree, fíjese en esto: Hoy en día, hasta los “hackers” más avanzados evitan perder tiempo y esfuerzo en violar los sistemas de seguridad de la banca. Los desarrolladores de software de seguridad compiten en astucia con los intrusos informáticos y, por lo general, antes de que alguien encuentre una fisura en el sistema, ya se ha puesto en práctica la medida de seguridad que la corrige.

Esta es la explicación por la que, quienes tienen intenciones maliciosas, enfilan sus baterías, no contra los sistemas de la banca, sino hacia las computadoras de los usuarios y los descuidos que pudieran cometer. Fraudes como el “phishing” (suplantación de identidad corporativa) o la captura ilícita de datos personales, claves secretas y otros, se enfocan en tratar de engañar, no al sistema, sino a las personas que lo utilizan.

Lo que quiere decir esto es que está de nuestra parte tomar las medidas de precaución necesarias para que la tecnología sea realmente invulnerable.

¿Cómo protegernos?

En ocasiones anteriores nos hemos referido a algunas de las recomendaciones básicas para realizar operaciones seguras de banca electrónica. Como sabemos, es fundamental resguardar nuestras claves secretas y datos personales, cambiar frecuentemente los datos de acceso al sistema, no compartirlos, enviarlos por e-mail o guardarlos en lugares fáciles de descubrir, dentro o fuera de la computadora. Las siguientes son algunas recomendaciones más avanzadas:

- En lo posible, no haga transacciones en computadoras públicas. Si se ve en la necesidad de hacerlo, debe primero informarse acerca de cómo borrar permanentemente su historial de navegación, formularios, claves, “cookies”, etc. La mayoría de los navegadores permiten hacer esto de manera muy sencilla.
- Incluso cuando se trate de su propio computador, preferiblemente no realice transacciones mientras esté conectado a una red wi-fi pública, como las que hoy en día están disponibles en bibliotecas, cafés, parques, etc.
- Esté al tanto de las actualizaciones de sus programas antivirus, es mucho más conveniente invertir en estos programas que facilitar el acceso de un intruso.

twitter: @josegrasso