Estafas virtuales: advierten que los bancos deben mejorar sus sistemas de seguridad

14/11/2023

Las estafas virtuales están a la orden del día. El ciberdelito o delito informático es un hecho recurrente que en Argentina afecta a miles de personas. Por eso, la emisora radial FM Vos 94.5 entrevistó a la especialista en Derecho Informático y Ciberdelitos, Bárbara Peñaloza, quien sugirió que los bancos deberían cambiar su sistema de seguridad ante esta modalidad delictiva.

«Aunque los sistemas de seguridad se han ido fortaleciendo durante los últimos años, de igual manera los delincuentes han ido rápidamente encontrando otras alternativas para acceder a las cuentas de las víctimas. Siguen apostando al engaño y al error humano. En ese sentido, es que falta una toma de acción

efectiva por parte de las entidades. El Banco Central ordenó que los bancos deben monitorear las cuentas y emitir alertas cuando hay movimientos extraños», explicó Bárbara Peñaloza ni bien comenzó la entrevista. «Muchas veces se solicita un préstamo preaprobado en nombre de la víctima que luego es transferido de forma inmediata a cuentas que no estaban asociadas. Por ello, hay que hacer foco en este tipo de cuestiones para justamente prevenir de forma correcta este nivel de estafa. En el 2021 el Banco Central también estableció que el préstamo debe acreditarse inmediatamente a través de datos biométricos, pero el sistema fue vulnerado porque no es la forma más efectiva», amplió. «Cuando la víctima detecta que ha sido engañada por un delincuente, inmediatamente hace la denuncia, entonces si le diéramos 48 horas a la víctima, esta podría avisarle al banco que no pidió el préstamo», prosiguió explicando. Después, comentó qué es lo que se puede hacer para mejorar el sistema de seguridad en relación a este tipo de estafa. «El Banco Central dice que lo ideal sería que si alguien, por ejemplo, quiere sacar un préstamo preaprobado en tu cuenta, el banco debería mandarte un mail o alerta que te diga que están queriendo sacar un préstamo a tu nombre. Con 48 horas, la víctima tiene la posibilidad de desconocerlo. Las medidas de seguridad ya están establecidas, lo que ocurre es que están mal utilizadas. Los delincuentes apuntan constantemente al error humano», subrayó Peñaloza. Más adelante advirtió sobre otros tipos de delitos informáticos. «En muchos casos ingresan a las cuentas de las víctimas a través de aplicaciones y manejan de manera remota el dispositivo. También pueden acceder a las cuentas a través de la implementación de algún virus que infecta el dispositivo en cuestión», recalcó la especialista en Derecho Informático. A su vez, indicó las razones por las cuales las entidades bancarias no extreman las medidas de seguridad. «Todo esto se encuadra en el marco de la inmediatez, la facilidad y la accesibilidad de operar online, todo con un click. Ahora bien, esas facilidades van en contra de la seguridad. En síntesis, las medidas extremas no van de la mano en lo que concierne a

la facilidad y el uso del sistema. Los bancos deberían tener un call center las 24 horas del día, del mismo modo que se puede operar online todos los días a cualquier hora y los 365 días del año», sostuvo la doctora Peñaloza. «Las claves token vinieron a solucionar un poco este tipo de inconvenientes con las estafas. Las medidas se han complejizado un poco más, pero no lo suficiente. Es necesario que el usuario a la hora de operar con la banca de forma online, lo haga de una manera segura. Los tribunales de Mendoza están llenos de casos por estafa de este tipo. El consumidor está expuesto a una vulnerabilidad, sobre todo en los préstamos preaprobados a los cuales las entidades bancarias los ponen como disponibles sin que el cliente los haya solicitado. La mayoría de la gente ni siquiera tiene conocimiento de esta posibilidad, porque los ciudadanos por lo general a la hora de pedir un préstamo lo hacen personalmente en una sucursal», aseguró al final de la charla.