El calvario de una mujer víctima de una ciberestafa: sacaron un crédito a su nombre y todos los meses le descuentan $40.000

29/10/2021

En enero de este año Leila Daleffe empezó a vivir un calvario. La venta de una mesa desató la estafa de la que fueron víctimas ella y su marido. Delincuentes hackearon sus cuentas bancarias y sacaron créditos con un solo click. La mujer hizo la denuncia, se presentó a mediaciones, tiene un abogado, pero hasta ahora, nueve meses después, sigue pagando por algo que no le corresponde.

En la publicación en Marketplace, ofrecía una mesa por $10.000. El domingo 17 de enero, una persona se contactó porque estaba interesada, sin sospechar que era un estafador siguieron la charla por privado donde le dio los datos para que haga la transferencia. Hasta ese momento iba todo dentro

de los carriles normales que hay en una transacción, pero una llamada telefónica fue el punto de partida del vía crucis que Leila transita hasta hoy.

El supuesto comprador le mandó un comprobante trucho donde le decía que le había transferido $100.000, mucho más de lo que Leila pedía por su mesa. A los pocos minutos la llamó **llorando** porque se había equivocado en el monto. "La verdad es que le creí por eso **no entré a mi cuenta bancaria para verificarlo.** Fue todo muy raro. Las cuentas fueron bloqueadas, y más tarde me llamaron para decirme que eran del banco para solucionarlos y les di los datos. Pero también era mentira. Con esos datos sacaron dos créditos, uno de ellos lo sigo pagando hasta hoy", contó

Con toda la información que necesitaba, el delincuente pudo ingresar a la **cuenta sueldo del Banco Nación de Leila y a otra del Banco Patagonia** que tiene en común con su esposo. En el primero sacó un **crédito de $600.000 y en el segundo de $200.000.** "La gente del Patagonia se portó muy bien y actuó rápido, reconocieron todo y el problema quedó solucionado, pero los del Nación nada que ver. Tuve que poner un abogado y nadie me puede explicar cómo le dieron un crédito a una persona **sin acreditar la identidad".**

A las horas Leila quiso entrar a las cuentas y ambas estaban **bloqueadas**. Dañada en su confianza, lo único que se le ocurrió fue llamar al **911.** La policía fue hasta su casa y le indicaron que hiciera la denuncia en la comisaría correspondiente. Al día siguiente, el caso ya estaba en manos de los policías de **ciberdelito quienes identificaron que la estafa venía de presos alojados en cárceles de Córdoba**. "Transfirieron toda la plata a 15 cuentas distintas".

A pesar de estar localizados, el calvario de Leila no terminó. "Tenemos toda las pruebas pero el banco Nación se **niega a devolverme lo que es mío**. No reconocen que fui estafada y que en realidad el error es de ellos, porque le otorgaron un

crédito a un delincuente con un sólo click”.

Lo cierto es que a la mujer **todos los meses le descuentan $40.000.** El crédito fue sacado en **36 cuotas**, y si no le solucionan el problema va terminar **pagando más de $1 millón que nunca pidió prestados.**

Unos meses después de lo que le pasó a Leila y ante la creciente ola de ciberestafas, el Banco Central (BCRA) reforzó las medidas de seguridad que deberán tomar las entidades financieras a la hora de otorgar estos préstamos preacordados a través de canales electrónicos, una de las principales vías de las que se aprovechaban criminales informáticos.

A partir de ahora, los bancos deberán verificar fehacientemente -ya sea a través de llamado telefónico, reconocimiento facial o cualquier otra técnica de identificación positiva- que efectivamente es el cliente quien está solicitando el préstamo que la entidad le tiene asignado de acuerdo a su categoría crediticia.

Como segunda barrera de control, una vez verificada la identidad del cliente, la entidad deberá comunicarle “a través de todos los puntos de contacto disponibles” que su crédito se encuentra aprobado y que, de no mediar objeciones, **el monto será acreditado en su cuenta recién a partir de las 48 horas hábiles siguientes.**

Los bancos también deberán hacer un monitoreo y control de, como mínimo, los puntos de contacto indicados por el usuario y comprobar que no hayan sido modificados recientemente, de modo de detectar posibles engaños o robos de claves.

Fuente: TN