FUNDAMENTOS

Se denomina home banking, banca online o e-banking, a los servicios bancarios a los que se puede acceder a través de internet por medio de computadoras, tablets o teléfonos celulares. Es necesario ser titular de una cuenta bancaria, para poder operar a través de ésta modalidad, por la cual es posible transferir dinero a cuentas propias o de terceros, ver su resumen de cuenta y consultar su saldo, pagar impuestos y servicios, tomar un préstamo, realizar inversiones, realizar pedidos de chequeras y boletas de depósito, consultar el CBU de su cuenta, dar aviso de viajes, consultar saldo de tarjetas de crédito y en general, interactuar con la entidad para realizar operaciones y administrar los servicios que brinda.

Las contraseñas deben ser seguras y deben ser modificadas periódicamente. Hay que tener en cuenta que sean difíciles de adivinar y fáciles de recordar. Esa clave no debería ser ni la fecha de nacimiento ni el domicilio personal u otro número que pueda conseguirse simplemente de documentos que se guarden en el mismo sitio que la tarjeta.

Los bancos no envían correos electrónicos, ni realizan llamadas telefónicas para solicitar cambio o confirmación de datos personales (número de cuenta, nombre de usuario, clave de accesos o datos de tarjetas de coordenadas). Estas suelen ser prácticas utilizadas para obtener datos que permitan el robo de identidad. Para mayor seguridad de que se está conectando con el sitio correcto en la página de acceso al Home Banking, no hay que ingresar al banco a través de direcciones o links que se reciban por correo electrónico o ventanas emergentes. Para algunas operaciones, las más riesgosas, son utilizados los denominados factores de "doble autenticación", como tarjetas de coordenadas o tokens. En general estos elementos se solicitan a la entidad y se activan a través de cajeros automáticos.

El fraude y estafa en cuentas bancarias, como el robo de claves de acceso a home banking o de datos de tarjetas de crédito, fue uno de los delitos que más ha crecido últimamente. Las estafas pueden llegar a tener formas más o menos elaboradas pero, en todos los casos, se trata de estrategias con las que los delincuentes atraen la atención de usuarios de dinero digital para hacerse de datos personales y, entonces, robarles dinero, hacer consumos con sus tarjetas o pedir préstamos de rápido otorgamiento.

Desde entonces arreciaron casos de personas con cuentas bancarias o tarjetas de crédito asociadas contactados por delincuentes a través de redes sociales, correo electrónicos o hasta llamados telefónicos para ofrecerles supuestas promociones exclusivas, la solución a un inconveniente operativo o hasta regalos o beneficios especiales.

Uno de los principales cambios que deja la pandemia es el salto en bancarización de usuarios que, por ejemplo, crearon millones de nuevas cuentas para acceder a los programas como el Ingreso Familiar de Emergencia (IFE) o que comenzaron a usar billeteras digitales para pagar consumos cotidianos.

En los últimos meses, tanto el Banco Central (BCRA) como las principales entidades bancarias del país trabajaron en campañas de concientización conjunta para aconsejar a los usuarios financieros de modo que eviten caer en ciberataques. La clave, insisten desde el sector financiero, es que la gente advierta que compartir claves o gestionar nuevas por pedido de un supuesto representante del banco es algo muy peligroso.

Entre los consejos más simples pero imprescindibles están: no dar datos confidenciales por teléfono, correo o SMS; ingresar siempre al home banking a través de la página oficial del banco y no por un buscador; nunca ir a cajeros automáticos si lo piden por teléfono; verificar que las cuentas de redes sociales de los bancos cuenten con un tilde azul de validación.

En varias de las provincias de Argentina se han planificado y ejecutado programas de concientización, desde las autoridades gubernamentales, respecto a esta modalidad delictiva. Se lanzaron campañas mediáticas y en las redes sociales con varios spots, donde de manera sencilla y didáctica se alerta a la población en la prevención y el procedimiento a seguir; en caso de haber sido víctima de ese delito. Se recomienda no aportar datos personales, ni de cuentas bancarias a personas que no conozcan o ajenas a su círculo familiar.

Distintos organismos públicos, entre ellos la Defensoría del Pueblo de la ciudad Autónoma de Buenos Aires y la defensoría del pueblo de la ciudad de Neuquén, han intervenido en esta problemática.

El titular del Juzgado Civil N°1 de Cipolletti le ordenó al Banco Patagonia que se abstenga de realizar el débito de la cuota prevista para el mes de mayo de 2021, por la suma de 26.000 pesos como así también de las sucesivas, relacionadas con el préstamo cuestionado y se abstenga igualmente de informar la supuesta deuda al sistema de información crediticia, hasta que se resuelva la cuestión de fondo.

La primera de las 60 cuotas del préstamo venció en mayo y la abogada consiguió un freno legal antes del primer débito. Además por el beneficio de justicia gratuita contemplado en la ley de Defensa del Consumidor la jubilada fue eximida de presentar contracautela (una garantía) al momento de la solicitar la medida cautelar de no innovar.

La situación se inició el 1 de abril pasado cuando la mujer recibió un llamado telefónico de un supuesto gerente de premios de un supermercado de la región. Con la excusa de acreditarle el dinero que había ganado en ese sorteo le pidió a la jubilada que generara un ticket en el cajero del Banco Patagonia. Con esa maniobra, la hicieron incurrir en un error.

El lunes siguiente, luego del feriado, la mujer advirtió que tenía un débito de 500 mil pesos. Cuando indagó descubrió un préstamo por 420 mil y ese dinero - junto con el que tenía en su caja de ahorros producto del sueldo de Anses - había sido transferido a otra cuenta.

En consecuencia hizo la denuncia en la Fiscalía de Cipolletti donde se inició una investigación por estafa. Luego su

abogada presentó el pedido de la medida cautelar de no innovar ante el fuero Civil. El préstamo tomado es por el plazo de cinco años, con un descuento en el haber jubilatorio de 26 mil pesos por mes.

El juez que resolvió afirmó que no hay dudas de la existencia de un contrato de consumo, de modo que los principios de protección del consumidor guiarán la apreciación del caso. "En tal sentido, la parte más débil de la relación es la aquí actora en tanto destinataria de la utilización de un sistema diseñado por la entidad bancaria, sobre quien pesa el despliegue de todas las salvaguardas que doten de confiabilidad al mismo para su operación electrónica o digital (cajeros automáticos o homebanking)", establece la resolución.

El Estado debe intervenir inmediatamente ante esta problemática que ya ha afectado a numerosos vecinos de diferentes ciudades de la provincia. En función de ello debe trazar estrategias a través de sus organismos competentes para que trabajen en forma articulada con el objeto de prevenir esos hechos.

Por ello;

Autor: Luis Ángel Noale.

LA LEGISLATURA DE LA PROVINCIA DE RIO NEGRO

COMUNICA

Artículo 1°.- A las autoridades del Banco Patagonia S.A., Agente Financiero de la Provincia, la urgente necesidad de instrumentar los mecanismos que considere adecuados, con el objeto de:

- a) Fortalecer las medidas de seguridad informática interna, profundizar el sistema de seguridad de operación de su sistema de gestión, en lo referido al acceso remoto a las cuentas bancarias de sus clientes y al otorgamiento de paquetes de productos vía online, de modo de dar garantías de uso exclusivo de estas herramientas a titulares o personas autorizadas por los mismos.
- b) Coordinar acciones para que los cajeros automáticos no induzcan, a los clientes, directamente o indirectamente con publicidades de préstamos pre aprobados que puedan generar confusión.
- c) Generar canales y vías de atención prioritaria a los usuarios que denuncien haber sido víctimas de ciberdelitos, para tomar debido registro, brindarles asesoramiento apropiado y tomar medidas eficaces que permitan resguardar su patrimonio.
- d) Impulsar, la formalización de convenios de cooperación recíproca entre la entidad bancaria y las unidades fiscales especializadas en delitos informáticos, a fin de articular medidas que permitan prevenir, neutralizar e investigar la comisión de delitos informáticos y perseguir penalmente a sus autores

Artículo 2°.- De forma.