NEGRI & PUEYRREDON ABOGADOS

Montevideo 850 Piso:1
C1019ABR - Buenos Aires
Argentina
Tel: (54-11) 5556-8000
e-mail: np@negri.com.ar
web: www.negri.com.ar

DOS MINUTOS DE DOCTRINA
OTRO LENGUAJE PARA LA COMPRENSIÓN DEL DERECHO

Año XVIII Número 978

27 de agosto de 2021

TEORÍA Y PRÁCTICA DEL "PHISHING": LOS JUECES AMPARAN AL CONSUMIDOR

Ante un caso de "phishing" y el dilema de elegir entre la palabra del banco o la de su cliente, los jueces adoptaron una posición flexible en amparo del consumidor.

Algunas cuestiones previas: "phishing" quiere decir suplantación de identidad. Es una técnica fraudulenta usada por delincuentes informáticos para obtener datos confidenciales como las contraseñas y números de tarjetas de crédito de incautos usuarios de servicios bancarios "on-line".

Los delincuentes envían correos electrónicos falsos a sus víctimas como anzuelo para "pescar" la información confidencial. ("To fish", en inglés, es pescar. El fonema /ph/ (que suena como la efe) tiene posible origen en las iniciales de las palabras "password hunting" ("caza de contraseñas").

A diferencia de otros tipos de amenazas cibernéticas, dedicarse al "phishing" no requiere sofisticados conocimientos técnicos. Según los que saben, es la forma más sencilla de ciberataque pero también la más peligrosa y efectiva, ya que casi siempre el eslabón más débil de cualquier sistema de seguridad no es una posible falla del código informático, sino alguien asustado o presionado que omite verificar la procedencia de un correo electrónico.

El delincuente ataca la computadora (u "ordenador", en España) más vulnerable y potente: la mente humana, engañándola. Los ciberdelincuentes no explotan la vulnerabilidad técnica de los sistemas operativos de sus víctimas, sino que se basan en trucos simples: mediante un correo electrónico o un mensaje de texto, envían mensajes amenazantes. ¿Para qué perder tiempo intentando burlar sistemas de seguridad cuando se puede engañar a alguien para que entregue la llave de acceso?

Las víctimas, por temor a las consecuencias, bajan sus defensas y actúan precipitadamente. El mensaje o correo electrónico dirigido a la víctima le exige actuar de inmediato bajo la amenaza de sufrir graves consecuencias (sobre todo en su relación con la entidad financiera con la que aquella opera).

En el mensaje, el ciberdelincuente imita o suplanta la identidad del emisor (generalmente alguien que goza de la confianza de la víctima, como su banco, una empresa de compras en línea o un proveedor de servicios públicos). Cuando aquella "muerde el anzuelo", cliquea en un enlace falso que la redirige a un sitio que, a su vez, imita al legítimo.

Una vez allí se le pide a la víctima que "confirme" sus datos confidenciales (como su nombre de usuario y la respectiva contraseña), generalmente bajo la amenaza de perder

control sobre su cuenta o por motivos de seguridad interna de alguna institución vinculada con la víctima. El delincuente accede así a las cuentas bancarias o roba la identidad de la víctima y hasta puede vender sus datos en el mercado negro para que sea otro quien haga "la tarea sucia".

Para evitar el "pishing" conviene revisar los resúmenes de las cuentas de banco para detectar transferencias no autorizadas; no seguir instrucciones originadas en correos o mensajes cuyo remitente es desconocido o similar (pero no idéntico) al de las páginas oficiales del proveedor; sospechar de faltas de ortografía o de sintaxis inusuales en mensajes institucionales o ante la presencia de enlaces dudosos; dudar cuando el mensaje omite el nombre correcto del destinatario, solicita la introducción de datos personales o incluye una dirección de internet (url) aparentemente incompleta ("argentina.io") en lugar de la correcta "argentina.gob.ar.", etcétera.

Lo más sencillo es no contestar ni completar formularios enviados por destinatarios desconocidos, no responder correos, mensajes telefónicos o de otro tipo en los que se solicite información personal ni descargar archivos de origen desconocido.

Hasta aquí la teoría.

En la práctica, son frecuentes los casos en la Argentina en los que los bancos otorgan préstamos a sus clientes sin que éstos los hayan solicitado. Para usar los fondos, sólo basta con pedir su desembolso, lo que puede hacerse electrónicamente.

Los ciberdelincuentes, mediante el "phising", obtienen los datos necesarios para obtener el desembolso de esos fondos (haciéndose pasar por el cliente del banco) y su acreditación en la cuenta de un tercero que inmediatamente los extrae y desaparece.

Eso le ocurrió hace poco a Alejandra, clienta del Banco BBVA Argentina. Cuando se percató de lo ocurrido, se presentó ante la justicia y pidió, como medida cautelar, que el banco "se abstuviera de efectuar descuentos" sobre su cuenta, "vinculados con ciertos préstamos" que ella dijo que nunca solicitó.

El juez aceptó el pedido y ordenó al banco no debitar la cuenta de Alejandra.

El banco apeló. Dijo que "no se encontraba debidamente acreditada la verosimilitud del derecho en virtud del cual se procede cautelarmente". Mas aún: agregó que la medida pedida por Alejandra le impedía "el legítimo derecho al cobro de los préstamos otorgados".

La "verosimilitud del derecho" es uno de los tres requisitos necesarios para pedir una cautelar. Los otros dos son el peligro en la demora y el otorgamiento de una garantía para el caso que la medida cautelar cause perjuicios.

La Cámara de Apelaciones[1] analizó primero la existencia de la verosimilitud. Dijo que "la contratación electrónica, con todos sus beneficios, conlleva también riesgos, que, en principio, *deben recaer sobre el banco,* que no solo es el creador del sistema, sino también quien lo administra en términos que deben garantizar a los usuarios la seguridad de las transacciones que se efectivizan en tal marco".

El tribunal se basó, entre otras, en una norma del Código Civil y Comercial según la cual "si las partes se valen de técnicas de comunicación electrónica o similares para la celebración de un contrato de consumo a

[1] In re "Koslowicz c. Banco BBVA Argentina SA", CNCom (C), exp. 6942/2021, 1CA1, 16 julio 2021; *ElDial.com* XXIII:5768, 25 agosto 2021, AAC615.

distancia, el proveedor debe informar al consumidor, además del contenido mínimo del contrato y la facultad de revocar, todos los datos necesarios para utilizar correctamente el medio elegido, comprender los riesgos derivados de su empleo y tener absolutamente claro quién asume esos riesgos".

Y aplicó también una regla clásica del derecho (cuyo texto permanece casi inmutable desde que Vélez Sarsfield lo incluyera en su glorioso Código Civil de 1869): "cuanto mayor sea el deber de obrar con prudencia y pleno conocimiento de las cosas, mayor es la diligencia exigible al agente y la valoración de la previsibilidad de las consecuencias".

Para el tribunal, "la asimetría informativa y de gestión entre las partes es notoria, lo cual ha llevado al legislador, ante situaciones que guardan sustancial analogía con la que aquí se verifica, a preferir al usuario aun cuando no haya ningún reproche subjetivo que pudiera ser efectuado al banco".

Los jueces pusieron como ejemplo de esa "preferencia" a favor del usuario de los servicios bancarios una disposición legal que prohíbe a los bancos cobrar los saldos deudores de tarjetas de crédito que han sido impugnados por sus titulares.

En rigor, la norma en cuestión permite a los bancos "cobrar sólo los saldos no impugnados de una tarjeta de crédito [por lo que] implícitamente le prohíbe cobrar los que sí lo están" aun cuando la impugnación no haya contado con prueba alguna.

Para el tribunal, esa disposición asume que la prueba para impugnar el saldo de la tarjeta de crédito "es de difícil o imposible producción inmediata, por lo que, a fin de evitar que sea el consumidor quien deba soportar las consecuencias de un eventual ilícito cometido por un tercero aprovechando los riesgos del sistema, acepta que, en esos supuestos se mantenga la situación preexistente a ese eventual ilícito".

De este modo, se evita que las derivaciones no queridas del hecho ilícito (del "phishing", en este caso) "recaigan sobre la parte más débil de las dos que deben considerarse igualmente víctimas".

Es decir que, aun cuando al banco no se le podía efectuar crítica alguna –pues la víctima del engaño no había sido éste sino Alejandra– en opinión de los jueces la mayor información y capacidad operativa del banco lo ponía en mejor situación para soportar las consecuencias de lo ocurrido (al menos mientras perdurara la medida cautelar).

Los jueces entendieron que "el peligro en la demora" (otro de los requisitos necesarios para decretar una cautelar) estaba implícito en la cuestión planteada: "la duda que genera el asunto debe, también aquí, ser resuelta a favor del consumidor".

Otro de los requisitos de la medida cautelar (la garantía o "contracautela") se dio por cumplido mediante el compromiso formal de Alejandra de asumir las consecuencias negativas que la medida cautelar podría eventualmente causar al banco.

La Cámara de Apelaciones, en consecuencia, confirmó la medida cautelar otorgada en primera instancia. Pero… ¿cómo seguirá la cuestión?

El Filosofito, que nos lee en borrador (y que a esta altura ha adquirido algunos rudimentos básicos de la ciencia del derecho) nos pregunta: "Cuando llegue el momento de la sentencia sobre el fondo del asunto –plazo durante el cual Alejandra no pagará intereses ni deberá devolver el capital del préstamo *que ella no solicitó pero que, con*

su falta de diligencia, ayudó a que se lo llevara un delincuente–, ¿el juez aplicará otro principio clásico según el cual *nadie puede alegar su propia torpeza*? Porque, después de todo, quien entregó la llave no fue el banco sino Alejandra…"

Para poder obviar su falta de diligencia, Alejandra debería poder demostrar la negligencia de parte del banco o de errores en el funcionamiento del sistema. Nada fácil, por supuesto.

* * *

Esta nota ha sido preparada por Juan Javier Negri. Para más información sobre este tema pueden comunicarse con el teléfono (54-11) 5556-8000 o por correo electrónico a np@negri.com.ar.

Este artículo es un servicio de Negri & Pueyrredon Abogados a sus clientes y amigos.
No tiene por objeto prestar asesoramiento legal sobre tema alguno.