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 XX Número 1133

22 de agosto de 2023

A LA PESCA DEL 'PHISHING'

Los jueces titubean ante los casos de fraude electrónico que afectan a los consumidores…
¡Y con razón!

Quizás sea necesario recordar algunas cuestiones previas acerca del 'phishing': básicamente se trata de una técnica de suplantación de la identidad de un cliente de un banco. La usan delincuentes informáticos que obtienen datos confidenciales (como claves de acceso y contraseñas de cuentas 'on-line') y números de tarjetas de crédito para defraudar a los incautos.

Hay muchas maneras de defraudar a los usuarios de servicios bancarios 'on-line': en algunos casos 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 'phishing' 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.

El caso de hoy presenta algunos aspectos novedosos: *el fraude no fue cometido mediante un ordenador o computadora personal sino a través de una aplicación telefónica que el cliente aseguró haber tenido siempre bajo su control.* Por eso el resultado fue diferente de otros casos analizados en ediciones anteriores[1].

Un día de abril de 2022, Ana, clienta del Banco de la Nación Argentina, ingresó a su *homebanking* y al ver los últimos movimientos en la cuenta advirtió que había un débito por alrededor de dieciocho mil pesos bajo la referencia de "débito-préstamo personal".

Como no entendió a qué crédito personal hacía referencia esa transacción, intentó comunicarse con el centro de atención del banco, pero le fue imposibe. Pocos días después fue a una sucursal del banco en Campo de Mayo, para que en la oficina de atención al cliente le explicaran qué era el débito en cuestión.

Según contó después, "en ese momento le informaron que correspondía a un crédito personal solicitado el 25 de febrero de ese año, por trescientos mil pesos". Como jamás había pedido un préstamo, "comenzó a desesperarse".

Le explicó al empleado que "al ingresar en su *homebanking* observaba transferencias a cuentas de terceros que tampoco había realizado".

Hizo entonces una denuncia ante el banco, en la que aclaró que no había solicitado ese préstamo ni había dado sus claves bancarias a sujeto alguno. Además, realizó una denuncia ante la comisaría de Bella Vista. Según Ana, "el banco no dio solución positiva a su reclamo".

Entonces inició pleito. En su opinión, "era evidente que alguien había ingresado en su

[1] "Teoría y práctica del 'phishing'", *Dos Minutos de Doctrina,* XVII:978, 27 agosto 2021; "No es fácil echarle la culpa al banco", *Dos Minutos de Doctrina,* XX:1112, 5 mayo 2023.

cuenta, solicitado un préstamo y robado el dinero en cuestión, habiendo sufrido una usurpación de identidad o que un empleado infiel del Banco Nación realizó un acto ilícito, con los serios perjuicios que ello le aparejó".

Exigió que se la resarciera por los daños sufridos y que se multara al banco por daño punitivo. Pidió también una medida cautelar urgente, que ordenara al banco no descontar ni debitar suma alguna de su cuenta bancaria, en relación al crédito otorgado sin su intervención.

El banco dijo que no estaba acreditada la verosimilitud del derecho invocada ni el peligro en la demora. Agregó que tanto el préstamo como las transferencias cuestionadas habían sido hechas no a través de la plataforma de *homebanking* sino desde la aplicación BNA+ en el dispositivo móvil de Ana. Por lo tanto fueron concretadas con acceso biométrico (ingreso por huella facial o reconocimiento dactilar) y un código ('PIN') generado por la propia usuaria.

El banco agregó que "la supuesta maniobra delictiva tuvo que contar necesariamente con la participación de Ana, al haber sido consumada desde la aplicación BNA+ instalada sólo en aparatos celulares, y no desde el *homebanking.* En consecuencia, "el pedido del préstamo cuestionado sólo pudo haber sido hecho mediante la validación de la operación con datos biométricos, por lo que cabía presumir la ausencia de participación de un tercero en su consumación". (Es decir, Ana había actuado sola).

En febrero de 2023, se rechazó la medida cautelar. Para la jueza de primera instancia, "era claro que parte de la pretensión sustancial coincidía con la medida cautelar solicitada, como así también que no concurrían circunstancias inminentes que, en caso de no accederse a la cautela pedida, condujeran a la configuración de extremos fácticos irreparables".

Por eso, "correspondía desestimar la medida requerida toda vez que, de accederse a ello, se desvirtuaría el instituto cautelar, por cuanto el objeto de la medida peticionada se confundiría con el resultado al cual se pretende arribar por medio de la sentencia definitiva, lo cual resultaba inadmisible".

Ana apeló. Entre otros argumentos, dijo que la jueza no había valorado que ella jamás pidió voluntariamente el préstamo (después transferido a cuentas de terceros) y que no se había evaluado el daño que le representaba el descuento mensual de las cuotas sobre su salario, indispensable para la manutención de su familia.

En segunda instancia[2], la Cámara dijo que una comunicación del Banco Central ("vigente desde el 25 de septiembre de 2021; esto es, antes de que tuviese lugar la operación cuestionada") establecía que "para la autorización de un crédito preaprobado [el banco] debe verificar fehacientemente la identidad de la persona usuaria de servicios financieros involucrada" y que "esta verificación debe hacerse mediante técnicas de identificación positiva".

El Banco Central exige, además, que previamente a través del resultado del proceso de monitoreo y control, como mínimo, se verifique que los puntos de contacto indicados por el usuario de servicios financieros no hayan sido modificados recientemente.

[2] In re "C., c. Banco de la Nación Argentina", CNCivCom Fed (III), exp.11509/2022/C2, 9 agosto 2023. *ElDial.express* XXV:6251, 15 agosto 2023, AAD90A

Una vez verificada la identidad del usuario, el banco deberá comunicarle –a través de algunos de los puntos de contacto disponibles– que el crédito se encuentra aprobado. De no mediar objeciones, el monto será acreditado en la cuenta del cliente en dos días.

Los bancos pueden obviar ese procedimiento si para autorizar un crédito preaprobado, verifican fehacientemente la identidad del cliente "mediante soluciones biométricas con prueba de vida". Además, están obligados a cancelar el crédito preaprobado y devolver las sumas involucradas y "anular los posibles efectos sobre la situación crediticia de la persona usuaria de servicios financieros" si ésta hace una denuncia policial dentro de los 90 días desde el vencimiento de la primera cuota del préstamo.

Ante la existencia de una norma semejante, el tribunal opinó que como el banco no aportó ningún elemento "demostrativo de la trazabilidad y verificabilidad de las operatorias de referencia" (como lo exige el Banco Central), debía "como lógica derivación, tenerse por demostrada *la verosimilitud de su derecho* esbozada por [Ana]".

La verosimilitud del derecho (uno de los dos elementos esenciales para que se otorgue una medida cautelar) se veía reforzada "por los elementos de convicción acompañados por [Ana] a la causa (denuncia e intercambio de *mails* con el banco, así como denuncia en sede policial, realizadas en forma coetánea a la toma de conocimiento de la ilicitud indicada)".

El tribunal puso énfasis en que la verosímilitud del derecho se refiere "a la posibilidad de que el derecho exista y no a una incontestable realidad, la cual sólo se logrará al agotarse el trámite judicial".

Además, la Cámara agregó que debía tenerse en cuenta "el carácter de consumidora que ostentaba [Ana] frente al banco, lo que, en principio, imponía una interpretación favorable a sus intereses".

Además de la *verosimilitud del derecho*, el otro recaudo que se exige para conceder una medida cautelar es el *peligro en la demora*.

Para el tribunal, éste consiste "en la neceéisdad de disipar un temor de daño inminente –acreditado prima facie o presunto–" y, en el caso, "era factible percibir los perjuicios que desde el plano económico le podría acarrear a [Ana] el devengamiento de las cuotas del cuestionado préstamo otorgado sin su consentimiento *–vgr*. ante una eventual mora por imposibilidad de pago–".

De modo que el tribunal entendió que "el peligro en la demora, en principio, también se encontraba acreditado y justificaba la concesión de la medida cautelar solicitada".

Un razonamiento (seguramente interesante) que introdujo el tribunal quedó opacado por la oscuridad con la que se lo expresó: "en virtud de la función preventiva del derecho de daños no es razonable advertir la continuidad de los perjuicios causados por una operación de crédito a la que la entidad bancaria permaneció ajena". ¿Qué se habrá querido decir?

Finalmente, el tribunal consideró el obstáculo planteado por "la coincidencia parcial de objeto entre la medida cautelar ahora dictada y la acción deducida", que generalmente impide su otorgamiento.

En el caso, los jueces entendieron que no se puede descartar la aplicación de las medidas cautelares "cuando existen fundamentos que imponen expedirse provisionalmente sobre la índole de la petición formulada. Ello es así

pues es de la esencia de estos institutos procesales enfocar sus proyecciones sobre el fondo mismo de la controversia, ya sea para impedir un acto o para llevarlo a cabo, pues se encuentran dirigidos a evitar los perjuicios que se pudieran producir en el caso de que no se dicte la medida, tornándose de dificultosa o imposible reparación en la oportunidad del dictado de la sentencia definitiva".

En otras palabras, las medidas cautelares deben ser "instrumentos jurisdiccionales tendientes a asegurar el resultado práctico de un proceso". El tribunal reconoció que "la medida requerida por [Ana] se erige, ciertamente, en *una decisión excepcional dentro del género cautelar porque altera el estado de hecho o de derecho existente al tiempo de su dictado*, ya que se configura un anticipo de jurisdicción favorable respecto del fallo final de la causa, mas no implica prejuzgamiento".

El tribunal entendió que la medida cautelar a favor de Ana "fundada en un análisis meramente liminar de la controversia, no importaba adelantar juicio sobre lo que pueda llegar a decidirse en definitiva al respecto", pues podría llegar a modificarse si se le suministraban nuevos "elementos de convicción".

Por consiguiente, se modificó la resolución de primera instancia y se otorgó la medida cautelar a favor de Ana, lo que le permitió dejar de pagar el préstamo hasta que la sentencia definitiva resolviera la cuestión (o el banco, con nuevos medios de prueba, demostrara que la medida debía ser modificada).

* * *

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.