ESTAFAS INFORMATICAS A CONSUMIDORES

Dra. Milagros Zannini

PANDEMIA : COVID 19

- Fuerte incremento de las relaciones de consumo celebradas a distancia, través de sistemas telemáticos.

- Fuerte incremento de “ciberataques” y fraudes electrónicos a través de técnicas de “Ingeniera Social”.

- Se ve exacerbada la vulnerabilidad de usuarios y consumidores.

MODALIDADES DE ESTAFAS INFORMÁTICAS SEGÚN EL MEDIO DE COMISIÓN.

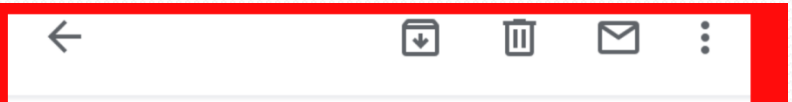
- **PHISHING:** "*password harvesting fishing*" *significa* cosecha y pesca de contraseñas. Esta tecnica Consiste en el envío de correos electrónicos fraudulentos que dirigen a los clientes a páginas web falsas que aparentan ser de una entidad oficial (Phishing Bancario). También pueden presentase en redes sociales como cuentas falsas que postean contenido fraudulento y solicitan información confidencial de los usuarios.

Defensa del Consumidor
GRAL. MADARIAGA

ALERTA PHISHING

EMAIL DE REMITENTE FALSO SUPLANTANDO LA IDENTIDAD DE VISA.

- NO SIGAS LOS PASOS INDICADOS EN ESE EMAIL.
- NO COMPARTAS TUS DATOS PERSONALES NI BANCARIOS.
- ANTE LA DUDA, PODES DIRIGIRTE AL BANCO EMISOR DE LA TARJETA Y CONSULTAR.



De: "Legales Visa." <steven.felts@xerox.com>
Fecha: 2 de diciembre de 2020, 05:41:50 ART
Para:
Asunto: Tarjeta y cuenta en el Veraz.

Cliente estimado , último aviso para usted. Debido a que se encuentra debiendo cuotas de su tarjeta , existe un credito impago. Estará siendo ingresado a la lista negra del veraz , por ende no podrá comprar ni debitar pagos automáticos de servicios.

Tiene disponibles los días anteriores al 5 de Diciembre para dirigirse a una sucursal de Pagofacil o Rapipago y cancelar los 4340 pesos del pago mínimo que le hemos asignado en promoción abonando de la siguiente manera: Deberá avisarle al cajero que realizará una carga de "MercadoPago" al siguiente número:

4 2 5 3 3 1 5 2 1 9

El cajero le comunicará que la cuenta está a nombre de Federico Fabián Mendez ,que es el gestor judicial de su cuenta , luego el cajero le preguntará su DNI y usted deberá dar el del titular de la tarjeta para así abonar los 4340 pesos del pago mínimo.

Usted es el único cliente deudor asignado a este gestor judicial con el monto de 4340 pesos , por lo tanto el pago impacta automaticamente y no es necesario mostrar el comprobante.

En caso de no realizar el pago mnimo hasta el 5 de Diciembre lo inhabilitaremos y su nombre se verá afectado en el veraz. Último aviso previo al juicio.

ALERTA PHISHING

Defensa del Consumidor
GRAL. MADARIAGA

MODALIDADES DE ESTAFAS INFORMÁTICAS SEGÚN EL MEDIO DE COMISIÓN.

- **VISHING:** deriva de la unión de dos palabras: *"voice"* y *"phishing"*. Esta técnica se realiza a través de llamados telefónicos, en general con información previamente obtenida (phishing), y utilizando mensajes alarmistas, se intenta de que el cliente revele el número de su clave o token digital, necesarios para autorizar transacciones

ESTAFAS TELEFÓNICAS

INGRESO FAMILIAR DE EMERGENCIA

Se han detectado llamados telefónicos y WhatsApp de falsos representantes de ANSES o supuestos gestores que ofrecen ayuda para cobrar el beneficio del IFE. De esta manera intentan robar tus datos personales y bancarios para tener acceso a tu caja de ahorro.
El trámite para obtener el IFE es personal y gratuito,no requiere realizar pago alguno.

NUNCA COMPARTAS TUS DATOS PERSONALES NI BANCARIOS POR TELÉFONO, WHATSAPP, NI A TRAVÉS DE INTERNET.
NO SABEMOS QUIÉN ESTÁ DEL OTRO LADO.

DEFENSA DEL CONSUMIDOR - GRAL. MADARIAGA

MODALIDADES DE ESTAFAS INFORMÁTICAS SEGÚN EL MEDIO DE COMISIÓN.

- **SMISHING:** fraudes o robo de datos cometidos a través de SMS, WhatsApp y otras aplicaciones de mensajería instantánea.

MENSAJE QUE CIRCULA A TRAVÉS DE WHATSAPP

OBJETIVO: CUENTA BANCARIA DEL CONSUMIDOR

- El **sujeto activo** toma contacto con su **víctima** a través de cualquiera de los medios mencionados, y logra engañarlo para que entregue **de manera voluntaria** información confidencial (claves de seguridad, datos de tarjeta de crédito, datos de cuenta bancaria y homebanking, usuarios y contraseñas, etc.).
- **Primer paso:** la víctima debe hacer inmediatamente la denuncia penal (¿es Hurto o Estafa?).
- **Segundo paso:** denuncia en Defensa del Consumidor.

APLICACIÓN DE LA LEY 24.240

- **BANCO:** Proveedor de servicios financieros (Art. 2° LDC).
- **VICTIMA:** Consumidor (Art. 1° LDC).
- **RELACIÓN DE CONSUMO:** el vínculo jurídico que une al Proveedor financiero –Banco- con la víctima de estafa informática –Consumidor- (Art. 3° LDC) .
- **ART. 1384° CCyCN:** *"Aplicación. Las disposiciones relativas a* ***los contratos de consumo*** *son aplicables a los* ***contratos bancarios*** *de conformidad con lo dispuesto en el artículo 1093".*

ACTUACIONES EN DEFENSA DEL COSUMIDOR

- Denuncia en Defensa del Consumidor.
- Banco presenta descargo deslindando responsabilidad.
- Se solicita al empleador el cobro por ventanilla (o cheque) hasta el Banco brinde medidas de seguridad suficientes.
- Se dicta MEDIDA PREVENTIVA (Art. 71 Ley 13.133).

ARGUMENTOS PARA LA MEDIDA PREVENTIVA

RESPONSABILIDAD DEL BANCO

- **Dueño o guardián** del sistema financiero informático.
- El propio Banco alienta a sus clientes a utilizar los sistemas telemáticos para realizar todo tipo de operaciones financieras (banca online).
- Contratos de adhesión.
- Generación de Confianza en sus clientes.
- In dubio pro consumidor.
- Perjuicio en los **intereses económicos** del consumidor.
- Responsabilidad **OBJETIVA**.
- **DEBER DE SEGURIDAD.**

DEBER DE SEGURIDAD EN LA LEY 24.240

- **ARTICULO 5º** — *Protección al Consumidor. Las cosas y servicios deben ser suministrados o prestados en forma tal que, utilizados en condiciones previsibles o normales de uso, no presenten peligro alguno para la salud o integridad física de los consumidores o usuarios.*

- **ARTICULO 6º** — *Cosas y Servicios Riesgosos. Las cosas y servicios, incluidos los servicios públicos domiciliarios, cuya utilización pueda suponer un riesgo para la salud o la integridad física de los consumidores o usuarios, deben comercializarse observando los mecanismos, instrucciones y normas establecidas o razonables para garantizar la seguridad de los mismos.*

COMUNICACIONES DEL BCRA

- **Comunicaciones A 3682 y A 4272 :** exige a los Bancos *"…tener implementado mecanismos de seguridad informática que garanticen la genuinidad de las operaciones".*

- **Comunicación A 6909 :** *"El sistema de débito directo no podrá ser utilizado para el cobro de cualquier concepto vinculado a préstamos".*

- **POR ELLO RESUELVO:**
- **ARTICULO 1º.- INTÍMOLE** a **BANCO … plazo perentorio e improrrogable de 5 (CINCO) DÍAS HÁBILES,** presente informe detallando en estas actuaciones, las medidas de seguridad desplegadas por la entidad a fin de corroborar la identidad del usuario que solicitó tanto los adelantos de haberes, como los préstamos, así como aquellas medidas tomadas a fin de garantizar fidelidad de las operaciones sobre la cuenta **N° XXXXXX titularidad de XXXXXXXXXXXX.** Asimismo, informe origen detallado del préstamo en cuyo descargo (ver fojas 9) manifiestan que *"no ingresaron las cuotas de préstamo por tener saldos insuficientes".*

- **ARTICULO 2º.- INTÍMOLE** a **BANCO …,** se abstenga de efectuar los descuentos sobre la cuenta N° XXXXXXX titularidad de XXXXXXXXXX**,** originados en préstamos, débitos y adelantos de haberes no autorizados ni adquiridos con el consentimiento de su titular.

- **ARTICULO 3°.-INTÍMOLE** a **BANCO …,plazo perentorio e improrrogable de 5 (CINCO) DÍAS HÁBILES** reintegre el dinero correspondiente a los descuentos ya efectuados por la entidad sobre la cuenta **N° XXXXXXXXX** titularidad de XXXXXXXX en virtud de los préstamos, débitos y adelantos de haberes no autorizados ni adquiridos con el consentimiento de su titular, y lo acredite en estas actuaciones.

REVOCATORIA PRESENTADA POR EL BANCO
ARGUMENTOS DE DEFENSA

- *"Las claves son confidenciales personales e intransferibles".*
- *"El resguardo de las mismas es exclusiva responsabilidad del titular".*
- *"Las transacciones fueron realizadas utilizando PIN y PIL correctos en primer intento".*
- *"Los préstamos **solicitados (?)** se encuentran vigentes a la fecha... El adelanto de haberes no es posible su reversión".*

- *Con relación al seguro de ATM…no se dará curso al reclamo dado que el hecho no se encuentra cubierto conforme lo expuesto en los términos y condiciones que rigen para el uso de la tarjeta".*

- *"…agravia que no haya considerado la* ***ruptura del nexo causal*** *por culpa de la víctima como eximente de responsabilidad".*

- *"…no habría mediado engaño en la obtención de la información".*

- *"…si todos los usuarios…con cuenta en la entidad…contrataran adelantos, o créditos y luego hacen una denuncia ante la Fiscalía con la* ***liviandad*** *de la Sra. XXXXX… y las autoridades de la OMIC dictaran una medida como la que aquí se cuestiona, seguramente mi poderdante ingresaría en una* ***crisis financiera…causando*** *un daño irreparable".*

- **<u>Recurso de Revocatoria:</u>** no se encuentra previsto en la Ley 13.133 contra medidas preventivas.

- Se eleva al Juzgado Contencioso Administrativo a fin de no afectar el debido derecho de defensa en juicio y revisión judicial suficiente.

- El Banco inicia un **Proceso Sumario de Ilegitimidad** (pretensión anulatoria).

JURISPRUDENCIA NACIONAL

- ***"Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos Aires"*** SENTENCIA 15 de Mayo de 2008, Camara Nacional de Apelaciones en lo Comercial, Capital Federal, CABA.
- ***"M. H. G. c/ Banco P.B.A. s/ Medidas Cautelares (traba/levantamiento)",*** de trámite, Juzgado Civil y Comercial N°25, La Plata (Expte. n° 25384).
- ***"Pedernera Juan Alberto c/ Banco de la Provincia de Buenos Aires s/ Nulidad de Acto Jurídico",*** de trámite, Juzgado Civil y Comercial N° 10, La Plata (Expte. 128367).

MADRID

- El Juzgado de Primera Instancia nº 48 fue el primer órgano judicial de España que se pronunció sobre la cuestión, el 27 de mayo de 2016.
- En su Sentencia condenó a Banco Santander a devolver a uno de sus clientes 55.275 euros que habían sido sustraídos de su cuenta corriente utilizando un virus informático
- *"**El banco es el responsable de velar por la seguridad del acceso al sistema de pago electrónico**, ya que era quien "tenía y disponía de los medios necesarios para detectar y evitar" los ataques mediante virus informáticos contra las cuentas de sus cliente"*

Algunas conclusiones…

- No son suficientes las simples **recomendaciones generales** de seguridad hacia los usuarios.
- El Banco debe asumir una **conducta activa** tendiente a evitar la generación de daños en los intereses económicos de los usuarios, atribuibles a los bienes o servicios que comercializan.
- No solo ocuparse de la prevención. Los bancos deben detectar estas situaciones y atacarlas.
- **Que los Bancos ANTES de autorizar préstamos, adelantos, etc. se comuniquen con el cliente para que pueda acercase a ratificar lo (DETECCIÓN Y RESPUESTA).**
- Autoridades de Aplicación Locales: tomar los reclamos (no sólo quedarse con la denuncia penal) ; dictar medidas preventivas; iniciar actuaciones de oficio; difusión de alertas.

DEFENSA DEL CONSUMIDOR
GRAL. MADARIAGA

CUIDADO!

ESTAFAS A TRAVÉS DE LLAMADOS O MENSAJES TELEFÓNICOS

Si te llaman avisándote que ganaste un premio en un sorteo del que nunca participaste, haciéndose pasar por empleados de diferentes organismos (ANSES, IPS, etc), para venderte productos, NUNCA compartas tus datos personales o bancarios, ni deposites dinero a una cuenta extraña, SIEMPRE Y ANTED QUE NADA solicitá los datos de la empresa (razón social, CUIT, domicilio legal) y con ellos concurrí a nuestras oficinas para asesorarte sobre quién está del otro lado


Defensa del Consumidor
GRAL. MADARIAGA
NO GANASTE UN PREMIO!
NO ATIENDAS LLAMADOS DE NÚMEROS DESCONOCIDOS.
SI ATENDÉS Y TE SOLICITAN TUS DATOS PERSONALES O
BANCARIOS CORTÁ LA COMUNICACIÓN INMEDIATAMENTE
ENGAÑO
Si no participaste de ningún sorteo desconfia de haber ganado un premio sin motivo.
NO COMPARTIR INFORMACIÓN
No compartas información personal ni bancaria sin saber quién está del otro lado
NO VAYAS AL CAJERO NI TRANSFIERAS DINERO
En el caso de ser ganador de un sorteo nunca te pedirán que deposites dinero en ninguna cuenta.

Defensa del Consumidor
GRAL. MADARIAGA

¡ALERTA PHISHING!

CAMUZZIGAS INFORMA QUE LA PROMOCIÓN DIFUNDIDA POR FACEBOOK ES TOTALMENTE FALSA.

INGRESANDO AL LINK PUBLICADO REDIRECCIONAN AL USUARIO A UN FORMULARIO PARA COMPLETAR DATOS PERSONALES Y BANCARIOS.

LAS NOVEDADES Y/O PROMOCIONES SE DIFUNDEN EN WEB Y REDES SOCIALES OFICIALES DE CAMUZZIGAS.

NUNCA BRINDES TUS DATOS PERSONALES, BANCARIOS NI CLAVES DE SEGURIDAD A TRAVÉS DE INTERNET, REDES SOCIALES, WHATSAPP NI TELEFÓNICAMENTE.

| FALSO |


Gracias