

PROPOSICIÓN CON PUNTO DE ACUERDO POR EL QUE SE EXHORTA RESPETUOSAMENTE A LA COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS (CONDUSEF) A QUE IMPLEMENTE UNA ESTRATEGIA DE COMUNICACIÓN Y PUBLICIDAD PARA LA PREVENCIÓN DE FRAUDES Y USO INDEBIDO DE TARJETAS DE DÉBITO Y CRÉDITO, ASÍ COMO LA ACTUALIZACIÓN DE CIFRAS SOBRE EL NÚMERO DE FRAUDES QUE SE HAN REALIZADO A PARTIR DEL MES DE MARZO DEL 2020.

El suscrito, Diputado Raúl Eduardo Bonifaz Moedano, integrante del Grupo Parlamentario de Morena, en la LXIV Legislatura del Honorable Congreso de la Unión y con fundamento en lo dispuesto en los artículos 58 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, somete a consideración de esta Honorable Asamblea, la siguiente Proposición con Punto de Acuerdo por el que se exhorta respetuosamente a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF, a que implemente una estrategia de comunicación y publicidad para la prevención de fraudes y uso indebido de tarjetas de débito y crédito, así como la actualización de cifras sobre el número de fraudes que se han realizado a partir del mes de marzo del 2020, al tenor de la siguiente:

Exposición de Motivos:

Las ventajas que ofrece el mundo digital también pueden ser usadas con fines negativos. Las modalidades de fraude electrónico son variadas, pero se pueden prevenir si uno se mantiene informado y toma medidas básicas. Recientemente se han conocido algunos casos de "vishing", estafa que se caracteriza porque los delincuentes utilizan una voz automatizada semejante a la de los bancos para robar información confidencial de los clientes.

Los diferentes medios electrónicos para poder acceder a nuestros trámites bancarios dejan en claro que facilitan nuestros movimientos económicos ante esta pandemia que se vive en el mundo entero, sin embargo pocas personas son las que se encuentran informadas de las diversas formas de fraude que se realizan, por ello es importante que los usuarios de las tarjetas de débito y crédito estén informados de todas las herramientas que se tienen para poder blindar sus tarjetas.

Ante ello, debemos tener claro que el **Phishing** es un término informático que denomina a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza y haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace)¹, de ello se deriva el smishing y vishing.

El **smishing** (de *Smishing*; a su vez, de *SMS* y *fishing*) es un nuevo tipo de delito o actividad criminal a base de técnicas de ingeniería social con mensajes de texto dirigidos a los usuarios de telefonía móvil. Se trata de una variante del *phishing*².

Bancomer define el "vishing" como un tipo de estafa que se realiza a través de llamadas telefónicas y que busca obtener información bancaria confidencial de las personas. El "modus operandi" del delito combina una llamada telefónica fraudulenta con información previamente obtenida desde internet. Su nombre proviene de la unión de las palabras: 'voice 'y 'phishing'.

En el mes de Marzo, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) emitió una alerta a la población sobre empresas gestoras de crédito que están ofreciendo préstamos exprés sin requisitos, como lo son comprobar los ingresos o consultar el Buró de Crédito del solicitante.

Condusef recordó que detrás de este tipo de llamadas existen delincuentes que buscan aprovecharse de los usuarios para cometer fraude, por lo que exhortó a no dejarse engañar y seguir las siguientes recomendaciones:

- No respondas llamadas o mensajes de correo sospechoso o remitentes desconocidos.
- Toma en cuenta que ni las entidades financieras, ni VISA o MasterCard u otro operador de tarjetas, solicitan datos personales a sus clientes o verificación de sus cuentas mediante correo electrónico, mensaje de texto

¹ Cómo saber cuándo un estafador se está haciendo pasar por tu banco. BBC News Mundo. 13 de febrero de 2019

² Smishing article at ConsumerAffairs.com

o vía telefónica, a menos que el usuario haya sido quien contactó primero a la institución financiera.

- Llama directamente a la institución bancaria ante cualquier duda.
- Evita proporcionar tu información financiera a desconocidos.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), da a conocer la actualización del Buró de Entidades Financieras al cierre del 2019, en donde las reclamaciones al Sistema Financiero alcanzan los 7.9 millones.

Del total de las reclamaciones presentadas por las personas usuarias de productos y servicios financieros durante el 2019, el 93.2%, es decir, 7 millones 415 mil 860, se realizaron al sector Bancario, fundamentalmente por la elevada transaccionalidad de los productos que opera; 171 mil 310 a SOFOM E.N.R.; 113 mil 886 al sector Asegurador, 91 mil 24 a SOFOM E.R.; 13 mil 934 a las SOFIPO; y 6,081 a las SOCAP.

Sin embargo, destaca que, mientras la CONDUSEF atiende directamente el 2% del total de reclamaciones que se presentan a los bancos, es decir, 2 de cada 100; en seguros la proporción es de 35 y en Afore se eleva hasta 56 por cada 100 reclamaciones, lo cual tiene su explicación por el tipo de producto financiero que ofrecen y al modelo de atención e infraestructura que cada uno de estos sectores tiene para atender a su propia clientela.

Las sanciones impuestas incrementaron 77% con un número de 10,262, mientras que el monto de sanción creció 87%, al registrar 482 millones de pesos.

Durante abril del 2018, CONDUSEF alertó a la población en general de un nuevo caso de “vishing” en nombre de la institución financiera BBVA Bancomer.

El boletín señalaba que era un nuevo modus operandi detectado por esta Comisión Nacional, el falso empleado de Bancomer se pone en contacto con el usuario y argumenta haber identificado cargos en su tarjeta de crédito por el pago de un seguro.

Al momento de entrar la llamada, aparece en pantalla el número telefónico real de Línea Bancomer de la Ciudad de México, incluso el estafador pide al usuario verificar que el número en pantalla sea el mismo que contiene su tarjeta de crédito en la parte posterior.

Además algunas denuncias presentadas, señalan que las llamadas son de las sucursales bancarias.

Es importante recalcar que este modo de operación se ha incrementado no solo en la Ciudad de México, sino también en los demás Estados; la desinformación de los usuarios permite que los fraudes sean cada vez más frecuentes.

Las campañas contra el vishing por parte de CONDUSEF se impulsaron en 2018, pero no se ha tenido mayor difusión para la distribución y prevención de campañas contra este tipo de fraude.

La CONDUSEF informó que en 2016 se registraron 113 mil 23 reclamaciones relacionadas a fraudes electrónicos contra personas y empresas³.

Y de este número, 95% correspondieron a *vishing* o *phishing*, lo cual significa que –al menos– 107 mil 372 personas fueron víctimas del robo de datos, números de cuenta, códigos de seguridad y claves personales, a través de engaños.

Indicó que, de acuerdo a las cifras disponibles, dichos fraudes implicaron un daño económico de alrededor de dos mil 35 millones de pesos durante el año pasado; de los cuales sólo se pudieron reponer o recuperar entre 3.7% y 12%.

"El 70% de quienes son blanco de vishing o pesca ilegal de datos financieros a través de llamadas telefónicas caen y son víctimas de fraudes, donde los delincuentes se quedan con toda su quincena o roban su identidad para contratar créditos a través de cajeros automáticos", alertó la Condusef.

³ <https://www.publimetro.com.mx/mx/noticias/2017/06/13/vishing-fraudes-telefonicos-se-dispara-20-mexico-condusef.html>

Asimismo, explicó que los fraudes por *vishing* o *phishing* tienen cinco facetas:

- Primera: llamadas telefónicas o envío de correos electrónicos a los usuarios de tarjetas de crédito o débito, donde los delincuentes se hacen pasar por empleados bancarios.
- Segunda: los supuestos agentes bancarios auguran que "el sistema" les arroja que hay una compra o intento de fraude por cantidades superiores a cuatro mil o 10 mil pesos; que el plástico está bloqueado o que alguien intento ingresar a sus cuentas desde otra ciudad o el extranjero.
- Tercera: los delincuentes proporcionan al cliente cuatro o seis dígitos de la tarjeta que tiene problemas, aprovechando que esos números se repiten en todos los plásticos emitidos en una misma ciudad y por el mismo producto –crédito o débito–, como si fuera un código postal.
- Cuarta: al percatarse que, efectivamente, la tarjeta tiene esos primeros números, el propietario accede a la solicitud de proporcionar el resto de los dígitos del plástico y claves de seguridad.
- Quinta: con dichos datos los agentes bancarios falsos realizan compras por Internet o vía telefónica de productos y servicios; y hasta contratan créditos en los cajeros automáticos, a través de la falsificación de la propia tarjeta

Siendo estos los datos más recientes con relación a este tipo de fraudes, resulta importante impulsar una campaña por los diferentes medios de comunicación sobre protección y blindaje a las tarjetas de débito y crédito, así como las formas de operación de los diversos tipos de fraudes existentes, lo anterior, para garantizar que la información llegue a todos los sectores de la población, ya que las campañas que se han presentado a través de las redes sociales, limitan el conocimiento de la información a los usuarios existentes en el país.

En virtud de lo anteriormente fundado y motivado, se somete a consideración de esta honorable asamblea la siguiente **PROPOSICIÓN CON:**

PUNTO DE ACUERDO

Primero.- La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) a que implemente una estrategia de comunicación y publicidad para la prevención de fraudes y uso indebido de tarjetas de débito y crédito,

Segundo.- La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) informe a esta soberanía la actualización de cifras sobre el número de fraudes que se han realizado a partir del mes de marzo del 2020.

Dado en el Salón de Sesiones de la Comisión Permanente del H. Congreso de la Unión a 05 de Junio del 2020.

ATENTAMENTE

**RAÚL EDUARDO BONIFAZ MOEDANO
GRUPO PARLAMENTARIO DE MORENA**