
PROPOSICIÓN CON PUNTO DE ACUERDO POR EL QUE SE EXHORTA RESPETUOSAMENTE COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS PARA QUE, EN EL ÁMBITO DE SUS ATRIBUCIONES, FORTALEZCAN Y AMPLIEN LAS ACCIONES DE PREVENCIÓN Y ATENCIÓN DE FRAUDES FINANCIEROS DURANTE LA PANDEMIA DE COVID-19, A CARGO DE LA SENADORA SASIL DE LEÓN VILLARD DEL GRUPO PARLAMENTARIO DEL PARTIDO ENCUENTRO SOCIAL.

HONORABLE ASAMBLEA

La suscrita, Senadora Sasil de León Villard, integrante del Grupo Parlamentario del Partido Encuentro Social y de la LXIV Legislatura, con fundamento en lo dispuesto en el artículo 58 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, en el artículo 8 numeral 1, fracción II y el artículo 276 ambos, del Reglamento del Senado de la República, someto a consideración del Pleno, la presente **proposición con punto de acuerdo por el que la Comisión Permanente del H. Congreso de la Unión, exhorta respetuosamente Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros para que, en el ámbito de sus atribuciones, fortalezcan y amplíen las acciones de prevención y atención de fraudes financieros durante la pandemia de COVID-19, al tenor de las siguientes:**

CONSIDERACIONES

Desafortunadamente, ante la pandemia de coronavirus COVID-19 personas dentro del crimen organizado han aprovechado la situación

para realizar intentos de fraude, principalmente relacionados con la venta de suministros médicos, ayuda en redes sociales para liquidar deudas y alertas de bloqueos o supuestas compras no autorizadas en tarjetas y cuentas bancarias, generalmente a través de medios electrónicos tales como mensajería instantánea, redes sociales o correo electrónico.

Si bien, los defraudadores han buscado y posiblemente seguirán buscando nuevas formas de estafar. Hoy lo hacen mediante el uso de sofisticadas tecnologías, a lo que se le conoce como fraudes cibernéticos. Con esta práctica no sólo pretenden obtener depósitos bancarios sino también robar datos personales y cuentas bancarias para saquearlas o realizar compras en línea.

Es por ello y ante la contingencia que se vive a nivel mundial por el COVID-19 que organismos internacionales han alertado sobre los riesgos de lavado de dinero, fraudes y robos de identidad que se pueden dar a partir de esta problemática.

Por ejemplo, para el Grupo de Acción Financiera de Latinoamérica (Gafilat), la preocupación está en las estafas, robo de información e incluso, actos de corrupción. En este sentido, el Gafilat prevé, un aumento de fraudes financieros y estafas, relacionadas con el tráfico de medicamentos falsos y ofertas de inversiones fraudulentas basadas en esquemas piramidales.¹

Otro ejemplo ha sido la Interpol, quienes hasta hace algunos días, habían detectado al menos 30 casos de posibles fraudes en Asia y Europa, lo que provocó el bloqueo de 18 cuentas bancarias y el

¹ GAFILAT, Comunicado Del Gafilat sobre COVID -19 y sus riesgos asociados de Lavado de Activos y Financiamiento al Terrorismo. Consultado en: <https://www.gafilat.org/index.php/es/espanol/19-noticias/102-comunicado-del-gafilat-sobre-covid-19-coronavirus>

congelamiento de 730,000 dólares por sospechas de transacciones fraudulentas. Inclusive el Secretario General de la Interpol, Jürgen Stock ha señalado que *“los delincuentes están explotando el miedo y la incertidumbre creados por COVID-19 para aprovecharse de ciudadanos inocentes que solo buscan proteger su salud y la de sus seres queridos”*.

Ante lo anterior, la Interpol emitió una alerta a sus 194 países miembros sobre los fraudes relacionados a la pandemia a fin de tomar medidas que ayuden a combatirlos y prevenirlos, enlistando una serie de recomendaciones generales para las naciones², tales como:

- Verificar independientemente la compañía / individuo que ofrece los artículos antes de realizar cualquier compra;
- Tener en cuenta los sitios web falsos ya que los delincuentes suelen utilizar una dirección web que parece casi idéntica a la legítima, por ejemplo, ‘abc.org’ en lugar de ‘abc.com’;
- Revisar las reseñas en línea de una empresa antes de realizar una compra;
- Tener cuidado si se le pide que realice un pago a una cuenta bancaria ubicada en un país diferente al de la empresa;
- Si cree que ha sido víctima de fraude, avisar a su banco de inmediato para que se pueda suspender el pago;
- No dar clic en enlaces ni abrir archivos adjuntos que no esperaba recibir, o que provengan de un remitente desconocido, y
- Tener cuidado con los correos electrónicos no solicitados que ofrecen equipos médicos o que solicitan su información personal para controles médicos.

² INTERPOL, INTERPOL avisa de una estafa relacionada con el COVID-19. Consultado en: <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/INTERPOL-avisa-de-una-estafa-relacionada-con-la-COVID-19>

Además, de lo anterior, el Observatorio de Delitos Informáticos de Latinoamérica (ODILA), ha destacado que existe una “cifra negra” en torno a la cantidad de estos crímenes, que realmente ocurren pero que no son tratados ni conocidos y, en consecuencia, a los cuales los Estados no dan ninguna respuesta. Según una investigación de ODILA, en 17 países de la región, el 83,6 % de los encuestados declararon no haber realizado nunca la denuncia tras ser víctimas de este tipo de delitos, pero, quizás más grave aún, es el hecho de que entre los que sí realizaron la denuncia, solo un 1 % declaró haber logrado una condena efectiva para los delincuentes.³

Actualmente en nuestro país hay más de 71 millones de usuarios en Internet, lo que significa que el uso cotidiano de esta plataforma, las redes sociales, y en general del ciberespacio, sea aprovechado por los delincuentes para cometer todo tipo de delitos.

Al respecto, datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) establecen que cada hora se cometen 463 fraudes cibernéticos en operaciones por comercio electrónico y banca móvil, ubicando a nuestro país, como el país que más fraudes cibernéticos registra en América Latina, por su mayor número de población y el crecimiento exponencial de sus operaciones en línea. Incluso ha reportado que de 2016 a 2019 se cometieron más 6 millones de fraudes, lo que obligó a este órgano descentralizado a lanzar el “Portal de Fraudes Financieros”⁴ para elaborar una base de datos y hacer más eficaz el combate de estos ilícitos.

³ ODILA. La Cifra Negra en los Delitos Informáticos. Consultado en: https://www.odila.org/pdf/cifra_negra_delitos_informaticos.pdf

⁴ CONDUSEF. Portal de Fraudes Financieros. https://phpapps.condusef.gob.mx/fraudes_financieros/index.php

Este sitio de enorme relevancia, cuenta con tres secciones:

- **Monitor de reportes:** En esta sección los usuarios podrán conocer los datos fraudulentos reportados, como: números de teléfono, páginas de Internet, correos electrónicos, instituciones falsas, entre otros. Asimismo, la forma en cómo se realizó el fraude con la descripción detallada del modus operandi.
- **Comparte tu experiencia:** Con un sencillo cuestionario, los usuarios podrán reportar los casos en los que fueron víctimas o bien, aquellos en los que identificaron un posible fraude al recibir un correo, llamada o mensaje de texto. Con esta información se ayuda a otros usuarios a prevenir algún tipo de fraude.
- **Infórmate y protégete:** A través de historietas, los usuarios podrán conocer cómo se llevan a cabo los fraudes financieros, sus diferentes formas y como evitarlos. Hallarán también información de Educación Financiera que la CONDUSEF ha desarrollado respecto al tema de fraudes.

Sin embargo debido a la apremiante situación se requiere mayor difusión de los contenidos de dicha plataforma, de manera que dicha información llegue a un mayor número de población en el menor tiempo posible. Es importante mencionar que el esfuerzo por prevenir los fraudes cibernéticos debe ser impulsado por todas aquellas áreas del Estado en sus distintos niveles de forma que se pueda lograr disminuir la incidencia de dichos delitos.

En este sentido, organismos como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, ha señalado que en México se han identificado campañas maliciosas que suplantan la identidad de autoridades gubernamentales, con el propósito de difundir noticias falsas como el pago de bonos semanales para la compra de alimentos ante la emergencia sanitaria o,

realizar estafas, redirigiendo al usuario a sitios web que facturan con anuncios. De ahí que el Instituto haya emitido recomendaciones en su sitio web⁵ para mantenerse alerta, identificar e ignorar los intentos de cibercriminales que pretendan realizar fraudes o difundir noticias falsas.

Si bien este problema no es novedoso, a nivel mundial ha aumentado a raíz de las medidas de aislamiento implementadas por los gobiernos, la desinformación y el miedo e incertidumbre. Desafortunadamente, durante la pandemia que enfrentamos, los clientes de la banca somos constantemente bombardeados en nuestras redes sociales y teléfonos con mensajes sobre supuestos bloqueos de tarjetas, compras no autorizadas o suplantación de identidad; cuyo fin es robar claves bancarias, datos personales y dinero.

Después de que la emergencia sanitaria pase y las actividades económicas se reactiven, las entidades financieras y la expansión del crédito serán clave para la recuperación económica, y lograr que los usuarios confíen en las instituciones será fundamental para lograr esto.

Por ello la urgente necesidad de ampliar y promover las acciones de prevención de fraudes electrónicos a través de campañas de concientización con información verás y completa a través de la cual los ciudadanos conozcamos el tipo de amenazas a los que nos enfrentamos en Internet y cómo muchas de ellas pueden ser prevenibles fácilmente al prepararse y mantenerse alerta.

Por lo anteriormente descrito, y con fundamento en lo dispuesto en las disposiciones señaladas, someto a consideración de esta Soberanía, la siguiente proposición con punto de acuerdo:

⁵ INAI. Portal de Datos Personales Seguros. <https://micrositios.inai.org.mx/covid-19/>

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) para que, en el ámbito de sus atribuciones, fortalezca y amplíen las acciones de supervisión, inspección y vigilancia a los usuarios de tarjetas de crédito, ante el posible aumento de fraude cibernético durante la pandemia de COVID-19, con el objeto de garantizar la protección y defensa de los usuarios.

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) para que, en el ámbito de sus atribuciones, fortalezcan y amplíen las campañas de información y prevención sobre fraudes financieros a través de todos los medios posibles.

Dado en el Salón de Sesiones de la H. Comisión Permanente del Honorable Congreso de la Unión a los 06 días del mes de mayo de dos mil veinte.

Suscribe.

Senadora Sasil de León Villard
Coordinadora del Grupo Parlamentario de Encuentro Social