GOBIERNO DE LA
CIUDAD DE MÉXICO

SECRETARÍA DE GOBIERNO

DIRECCIÓN GENERAL JURÍDICA Y DE ENLACE LEGISLATIVO

Ciudad de México, a 22 de agosto de 2022

OFICIO NO. SG/DGJyEL/RPA/II/00281/2022

Dip. Héctor Díaz Polanco
Presidente de la Mesa Directiva de la
Comisión Permanente del Congreso
de la Ciudad de México
P r e s e n t e

Le saludo con respeto; y con fundamento en los artículos 26, fracción II de la Ley Orgánica del Poder Ejecutivo y de la Administración Pública de la Ciudad de México; 7, fracción I, inciso B) y 55, fracciones XVI y XVII del Reglamento Interior del Poder Ejecutivo y de la Administración Pública de la Ciudad de México; me permito adjuntar el oficio SSC/CGA/OACS/0612/2022 de fecha 19 de agosto de 2022, signado por el Asesor del Secretario de Seguridad Ciudadana de la Ciudad de México, el Lic. Pablo Sergio Ocampo Baeza, mediante el cual remite la respuesta al Punto de Acuerdo promovido por la Dip. Martha Soledad Ávila Ventura y aprobado por ese Poder Legislativo de esta Ciudad en su sesión celebrada el día 20 de julio de 2022, mediante el similar MDSPRPA/CSP/0946/2022.

Sin otro particular, reciba un cordial saludo.

Atentamente,
El Director General Jurídico y de Enlace Legislativo
de la Secretaría de Gobierno de la Ciudad de México

PRESIDENCIA DE LA MESA DIRECTIVA
II LEGISLATURA
2 3 AGO 2022
Recibió: Pamela
Hora: 10:16am

Lic. Marcos Alejandro Gil González
direcciongeneraljuridica@cdmx.gob.mx

C.c.c.e.p. Lic. Pablo Sergio Ocampo Baeza, Asesor del Secretario de Seguridad Ciudadana de la Ciudad de México.

Actividad	Nombre del Servidor Público	Cargo	Rúbrica
Validó	Mtro. Federico Martínez Torres	Director de Enlace, Análisis Jurídicos y Acuerdos Legislativos	
Revisó	Lic Nayeli Olaiz Díaz	Subdirectora de Atención y Seguimiento del Proceso Legislativo	
Elaboró	Lic. Luis Pablo Moreno León	Administrativo Especializado L	

GOBIERNO DE LA CIUDAD DE MÉXICO

SECRETARÍA DE SEGURIDAD CIUDADANA
COORDINACIÓN GENERAL DE ASESORES
OFICINA DEL ASESOR DEL C. SECRETARIO

SECRETARÍA DE GOBIERNO
GOBIERNO DE LA CIUDAD DE MÉXICO
19 AGO. 2022
DIRECCIÓN GENERAL JURÍDICA Y ENLACE LEGISLATIVO
RECIBIDO HORA: 16:34
RECIBE:

881

Ciudad de México, a 19 de agosto de 2022.
Oficio No. SSC/CGA/OACS/0612/2022

Asunto: Respuesta a Punto de Acuerdo.

LIC. MARCOS ALEJANDRO GIL GONZÁLEZ
DIRECTOR GENERAL JURÍDICO Y DE ENLACE LEGISLATIVO
DE LA SECRETARÍA DE GOBIERNO DE LA CIUDAD DE MÉXICO
PRESENTE.

Estimado Director General:

En atención a su oficio número **SG/DGJyEL/PA/CCDMX/II/000227/2022** de fecha 25 de junio de 2022, al que se adjunta el diverso **MDSPRPA/CSP/0946/2022**, signado por el **Dip. Héctor Díaz Polanco**, Presidente de la Mesa Directiva de la Segunda Legislatura del Congreso de la Ciudad de México, por el que se comunicó la aprobación del siguiente punto de acuerdo:

> ***"PRIMERO.-*** *Se exhorta respetuosamente a la Secretaría de Seguridad Ciudadana para que, a través de la Unidad de Policía Cibernética, continúe e incremente la difusión de campañas para alertar a la ciudadanía sobre los riesgos de fraude y de acoso cibernético". (sic)*

Al respecto, con fundamento en lo dispuesto por los artículos 34, apartado A, numeral 2 de la Constitución Política de la Ciudad de México; 1°, 3°, 5° y 7° de la Ley Orgánica de la Secretaría de Seguridad Ciudadana de la Ciudad de México; 1°, 2°, fracción VIII, 3° numeral 1, fracción I, inciso a), 4° y 19 fracción V del Reglamento Interior que rige la organización y funcionamiento de esta Dependencia y, en cumplimiento a la función de *"analizar e integrar la información, que permita atender los requerimientos, exhortos o planteamientos que formulen los Órganos Legislativos…"*, prevista en el Manual Administrativo de esta institución, publicado el 18 de marzo de 2021 en la Gaceta Oficial de la Ciudad de México, me permito proporcionar el siguiente:

INFORME

1. Con la reestructuración de esta institución a partir de la publicación de su nueva Ley Orgánica en el mes de diciembre de 2019 y la expedición de su nuevo Reglamento Interior, en vigor a partir del 1° de marzo de 2020, se creó y está en operación la Dirección General de Investigación Cibernética y Operaciones Tecnológicas, adscrita a la Subsecretaría de Inteligencia e Investigación Policial, lo que permitió fortalecer la operación de la Policía Cibernética. Este cuerpo especializado se encarga de atender reportes ciudadanos relacionados con incidentes cibernéticos, realizar monitoreo y patrullaje en redes sociales e internet abierta para identificar y mitigar posibles riesgos, así como crear contenidos enfocados a la prevención de delitos.

Berna No 18, Piso 1, col. Juárez,
Alcaldía Cuauhtémoc, C. P. 06600, Ciudad de México
Tel. 5552425100 extensión 5165
Correo electrónico asesores@ssc.cdmx.gob.mx

CIUDAD **INNOVADORA** Y DE **DERECHOS**

2. Ahora bien, a fin de alertar a la ciudadanía sobre los riesgos de fraude y de acoso cibernético, entre el 1° de enero al 31 de julio de 2022, la Policía Cibernética ha impartido más de 590 pláticas informativas en escuelas, oficinas y áreas públicas. Además, se han elaborado y publicado un número importante de ciberalertas, informando a la población sobre los peligros de descargar y utilizar aplicaciones de préstamos a través de la red pública de internet:

https://www.ssc.cdmx.gob.mx/comunicacion/nota/2452-la-policia-cibernetica-de-la-ssc-informa-sobre-los-riesgos-de-descargar-y-utilizar-aplicaciones-de-prestamos-traves-de-la-red-publica-de-internet

Recomendaciones

- Descargar y actualizar antivirus en todos los dispositivos móviles.
- Ser precavido con los permisos que se otorgan cuando se instala una aplicación, revisar términos y condiciones.
- Verificar que las aplicaciones de préstamos estén reguladas por la CONDUSEF.
- No confiar en la obtención de préstamos accesibles, con pocos requisitos y sin revisión de buró de crédito.
- Cuidado al compartir identificaciones o documentos oficiales, podrían ser víctimas de robo de identidad.
- Verificar el domicilio físico de la empresa y realizar llamadas telefónicas para conocer las condiciones crediticias.
- Evitar llenar formularios con datos personales, números de cuentas o tarjetas bancarias, sobre todo si son en ventanas emergentes.
- No proporcionar ningún tipo de anticipo económico a través de transferencias o depósitos a cuentas de terceras personas o intermediarios.

https://www.ssc.cdmx.gob.mx/comunicacion/nota/177-la-policia-cibernetica-de-la-ssc-alerta-la-ciudadania-sobre-los-riesgos-de-descargar-aplicaciones-y-ceder-permisos-para-acceder-informacion-personal

Recomendaciones

- Antes de descargar una aplicación verifica su calificación, así como los comentarios de los usuarios.
- Evita almacenar contenido multimedia de documentos o de tarjetas bancarias.
- Procurar acudir a instituciones financieras para cualquier solicitud de préstamo y corrobora su existencia ante la CONDUSEF.
- Instalar y mantener actualizado un antivirus en los dispositivos móviles y ordenadores.
- Evita ingresar credenciales o datos bancarios a un sitio web no verificado o mandarlos mediante mensajería instantánea, pues pueden ser utilizados por terceros.
- No dejarse engañar por promociones excesivas, servicios gratuitos o tasas de interés muy bajas.
- Restringir, bloquear o eliminar todo medio de contacto con los agresores.
- Evitar acceder a intimidaciones y amenazas.
- No contestar llamadas o mensajes de números desconocidos y, en caso de hacerlo, no proporcionar datos personales o bancarios.

Adicionalmente, en el marco de la 7ª Semana de la Ciberseguridad, se llevaron a cabo conferencias sobre los diferentes incidentes cibernéticos que ocurren en la red pública de internet, siendo uno de los temas centrales las aplicaciones de préstamo de dinero y los riesgos que existen al descargarlas.

3. Por otra parte, como se dio a conocer en la conferencia de prensa de fecha 18 de agosto del año en curso, como resultado de labores de investigación y de gabinete de la SSC, se ubicaron domicilios de empresas vinculadas con las aplicaciones de préstamos y que funcionan como *"Call Center"*, en las que se emplea a personas para efectuar llamadas telefónicas y mensajes de cobranza, quienes para solicitar los pagos de los supuestos deudores, recurren a métodos de intimidación agresión psicológica y amenazas, que van desde las llamadas y mensajes constantes, hasta la difamación en redes sociales.

De igual forma, derivado de las funciones de monitoreo y también patrullaje virtual de la Policía Cibernética de esta institución, desde el año 2021 se detectaron a diversas empresas que por medio de plataformas, ofertan créditos en línea a través de aplicaciones para teléfonos móviles, los datos personales de los solicitantes se revisan con rapidez para ofrecerles una respuesta inmediata, los préstamos no tienen garantía alguna y las empresas cambian de nombre e identidad gráfica, debido a que no están legalmente constituidas, generando en ello confusión con los usuarios, porque después de un tiempo no es posible localizar la misma aplicación que utilizaron.

A través de este tipo de aplicaciones, que se descargan en teléfonos celulares, los préstamos o créditos se ofertan prácticamente sin requisitos y carecen de registro o control, lo que resulta muy atractivo para la ciudadanía, pero a cambio les solicitan permisos para acceder a la información personal que tienen almacenada en sus dispositivos móviles, tales como: agenda de contactos, contraseñas, ubicación, contenidos y galería de imágenes, que después son usadas para extorsionarlos.

Como parte de las labores para mitigar este tipo de actos delincuenciales, la Policía Cibernética de la Ciudad de México ha atendido 15 mil reportes por el uso de este tipo de aplicaciones, brindando asesoría y acompañamiento a los ciudadanos afectados para realizar la denuncia correspondiente ante el Ministerio Publico. En estos reportes se identificó que a las víctimas les enviaron imágenes y videos intimidantes para exigir el pago de los préstamos.

En septiembre del 2021, esta Secretaría presentó una noticia criminal en la Fiscalía General de Justicia de la Ciudad de México, a la que se integraron los reportes recabados y un listado de alrededor de 80 aplicaciones detectadas hasta esta fecha, incluyendo una cantidad importante de números telefónicos de los que provienen las llamadas de extorsión, así como los números de cuenta para el pago de los préstamos. En este año, se han elaborado al menos cinco noticias criminales asociadas a este tipo de aplicaciones.

En este contexto, con el objetivo de combatir las extorsiones de esta naturaleza, el 17 de agosto del año en curso, en coordinación con la mencionada Fiscalía, se desplegó un operativo para dar cumplimiento a órdenes de cateo en diferentes inmuebles identificados como instalaciones de las empresas vinculadas con las aplicaciones de préstamos y que funcionan como *"Call Center"*.

Los cateos se practicaron en doce domicilios ubicados en las alcaldías Cuauhtémoc, Benito Juárez, Coyoacán e Iztapalapa. Como resultado, se logró la detención de cinco presuntos responsables de origen asiático con residencia en el país y la desactivación de más de 90 aplicaciones de este tipo. De igual forma, se aseguraron más de 700 equipos telefónicos, más de 15 mil chips de diversas telefonías, más de 400 equipos de cómputo, dinero en efectivo en moneda nacional y extranjera, así como una cantidad importante de diversa documentación.

Informe que me permito someter a su consideración, para que por su amable conducto y de así estimarlo procedente de conformidad con las atribuciones de la Dirección General a su digno cargo, se remita al H. Congreso de la Ciudad de México, en la inteligencia que el uso y tratamiento de la información queda bajo la más estricta responsabilidad de dicho Órgano Legislativo.

Sin otro particular, aprovecho la ocasión para enviarle un cordial saludo.

ATENTAMENTE
EL ASESOR DEL C. SECRETARIO

LIC. PABLO SERGIO OCAMPO BAEZA

SECRETARÍA DE SEGURIDAD CIUDADANA
COORDINACIÓN DE

C.c.c.e.p.- **Comisaria Mtra. Patricia Herrera Rodríguez**, Coordinadora General de Asesores del Secretario de Seguridad Ciudadana de la Ciudad de México.- Para su superior conocimiento.- **cce-coordinacion-asesores@ssc.cdmx.gob.mx**
Acuse electrónico, fecha: _____, hora: _____, correo_____
Acuse electrónico de confirmación, fecha: _____, hora: _____, correo _____
C.c.c.e.p.- **Lic. María del Carmen Téllez Jiménez**, Coordinadora de Control de Gestión Documental del Secretario de Seguridad Ciudadana de la Ciudad de México. Para los efectos de registro.- **cceccgi@ssc.cdmx.gob.mx**.-
Folio: **SSC/CCGD/OP/27017/2022**
Acuse electrónico, fecha: _____, hora: _____, correo_____
Acuse electrónico de confirmación, fecha: _____, hora: _____, correo _____

De conformidad con los artículos 6 apartado A fracción II de la Constitución Política de los Estados Unidos Mexicanos, 2 fracción III, 3, 9, 23 y 31 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (LPDPPSOCDMX), los Sujetos Obligados deben garantizar la confidencialidad e integridad de los datos personales que posean, con la finalidad de preservar el pleno ejercicio de los derechos tutelados de sus titulares, frente a su uso, sustracción, divulgación, ocultamiento, alteración, mutilación, destrucción o inutilización total o parcial no autorizado. Por lo que el indebido uso por parte de las personas servidoras públicas respecto de los datos personales que con motivo de su empleo, cargo o comisión tengan bajo custodia, será causa de sanción por incumplimiento a las obligaciones de la LPDPPSOCDMX previstas en su artículo 127 fracciones III y VI.

Se hace constar que el presente documento ha sido elaborado conforme a las disposiciones jurídicas y administrativas aplicables, así como los soportes documentales que fueron proporcionados por las áreas correspondientes y realizados por los servidores públicos, cuyas iniciales y rúbricas se insertan a continuación.

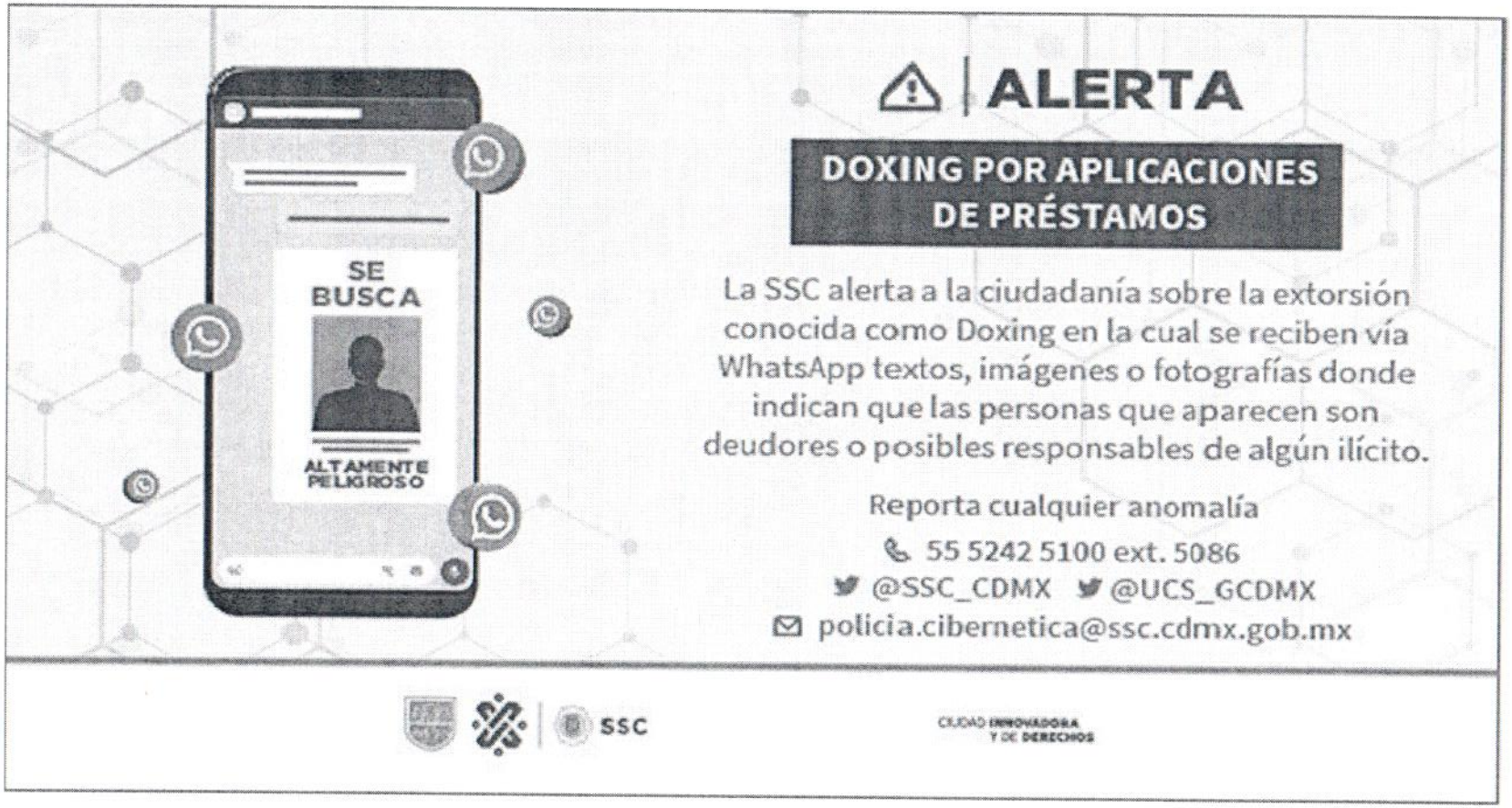
PSOB/CGSS/IJAM

OAE 0853/2022,OAE 0902/2022 y OAE 955/2022 (Concluidos)

EVIDENCIA DE ALERTAS PREVENTIVAS DE LA POLICÍA CIBERNÉTICA

Oficio No. SSC/CGA/OACS/0612/2022

"Alerta a la ciudadanía sobre los riesgos de descargar aplicaciones y ceder permisos para acceder a información personal".



EVIDENCIA DE ALERTAS PREVENTIVAS DE LA POLICÍA CIBERNÉTICA

Oficio No. SSC/CGA/OACS/0612/2022

"Alerta sobre falsos préstamos inmediatos ofrecidos a través de la red pública de internet".

⚠ | ALERTA

La Secretaría de Seguridad Ciudadana de la Ciudad de México alerta a la ciudadanía sobre **falsos préstamos** inmediatos ofrecidos a través de la red pública de internet.

En caso de ser víctima o testigo denuncia a través de:

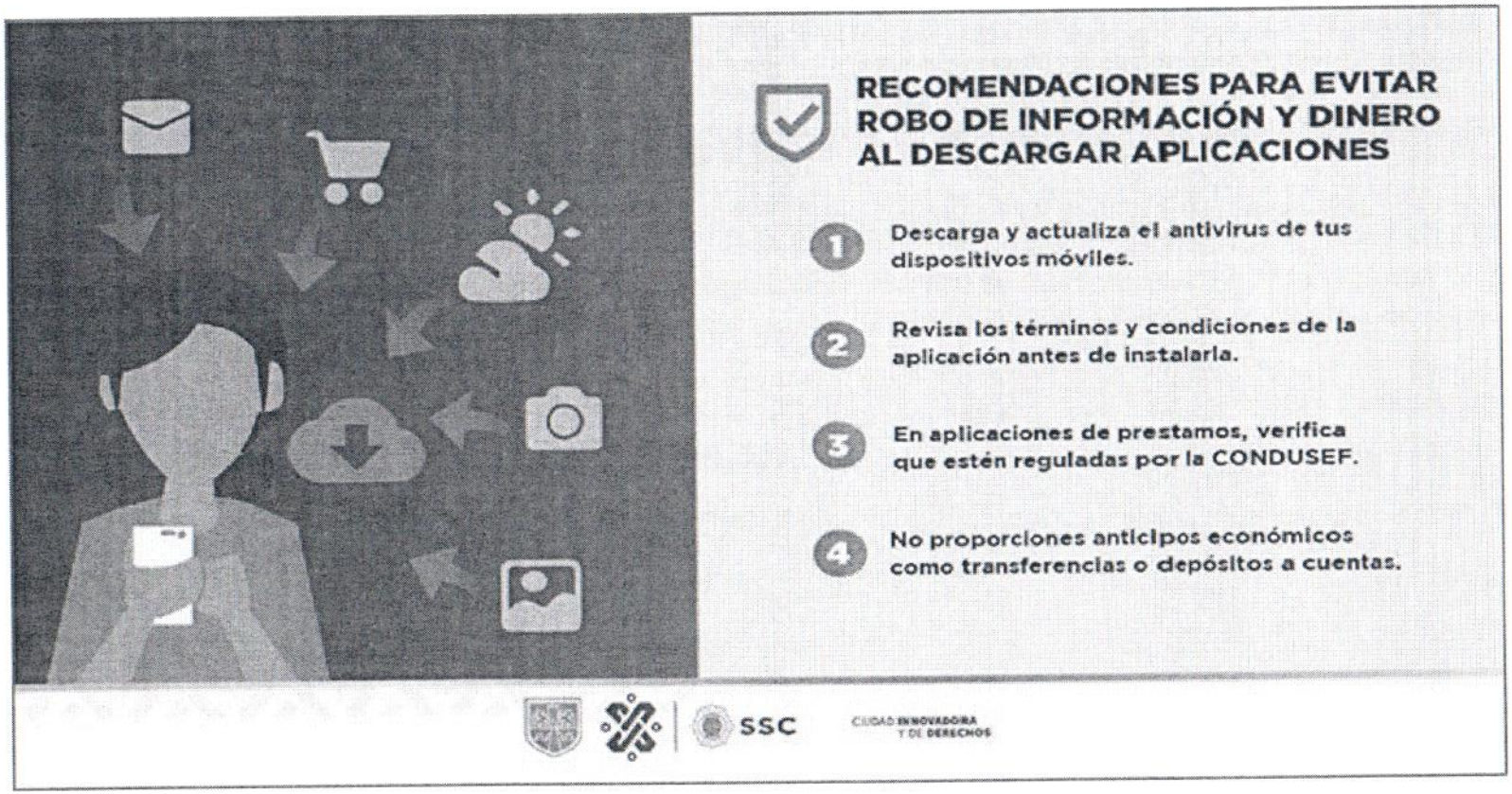
✉ **policia.cibernetica@ssc.cdmx.gob.mx**

✆ **55 5242 5100 ext. 5086**

EVIDENCIA DE ALERTAS PREVENTIVAS DE LA POLICÍA CIBERNÉTICA

Oficio No. SSC/CGA/OACS/0612/2022

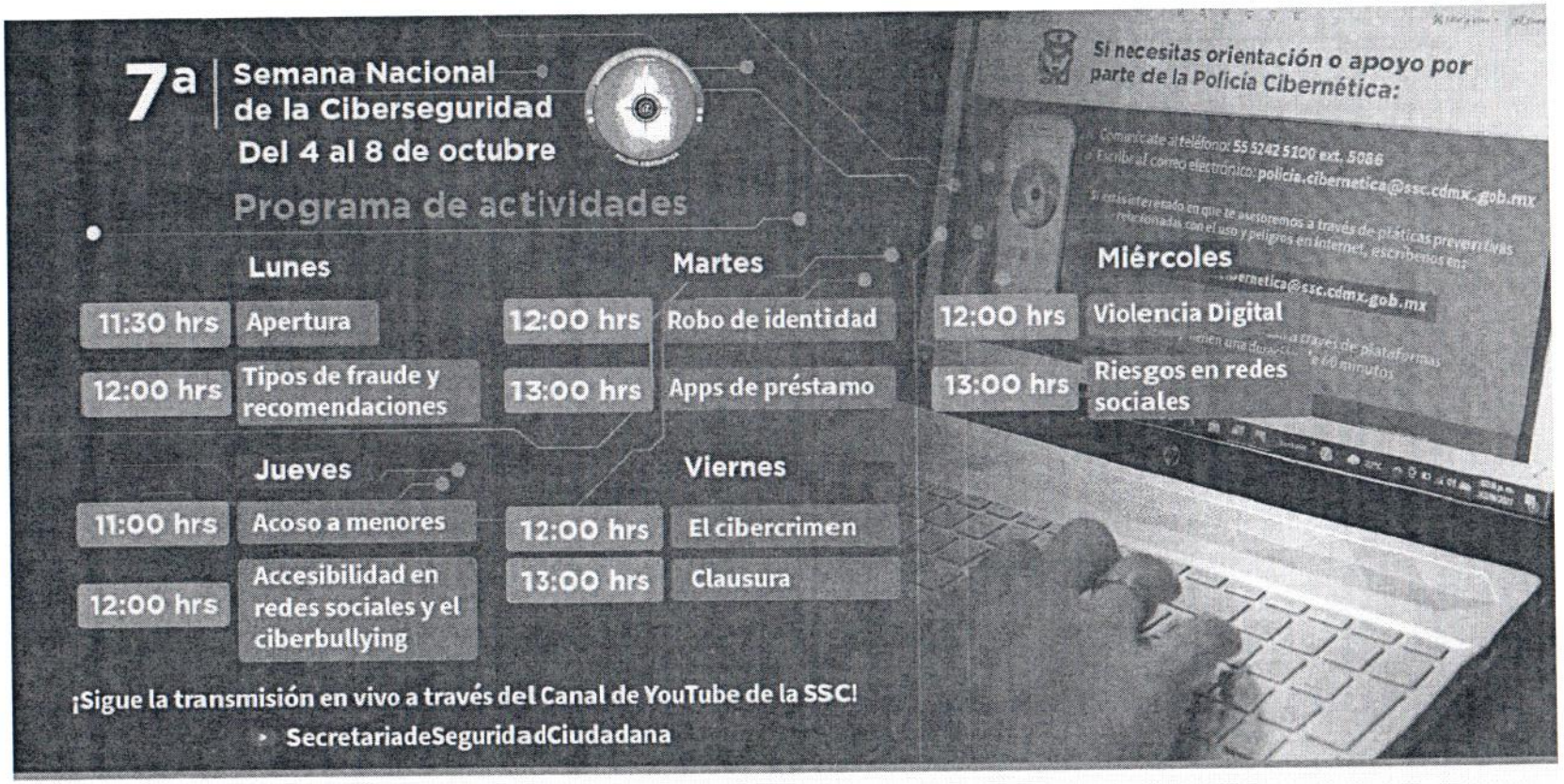
"Alerta sobre los riesgos de descargar y utilizar aplicaciones de préstamos a través de la red pública de internet".



EVIDENCIA DE ALERTAS PREVENTIVAS DE LA POLICÍA CIBERNÉTICA

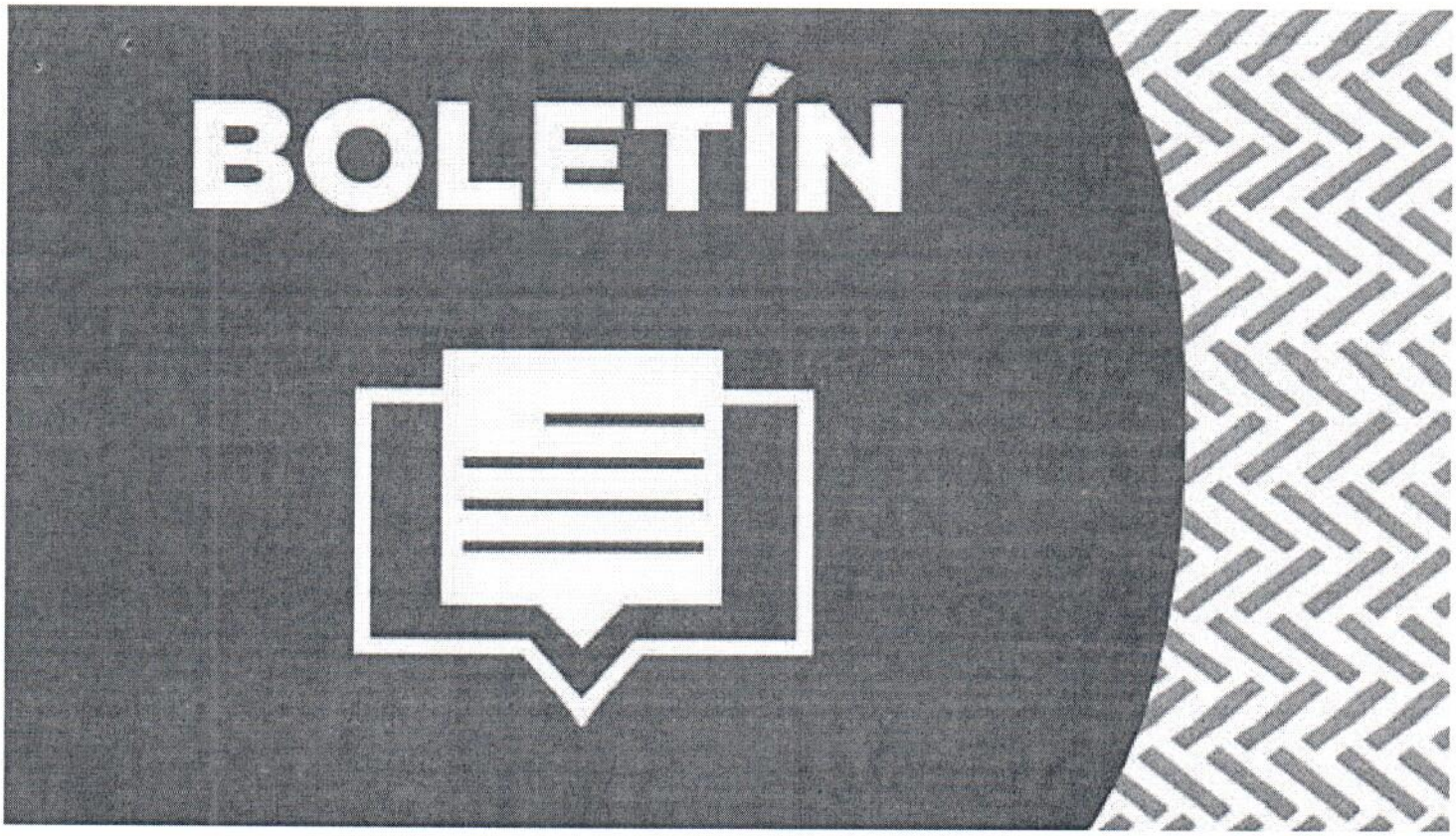
Oficio No. SSC/CGA/OACS/0612/2022

7ª. Semana de la Ciberseguridad



2452: La Policía Cibernética de la SSC informa sobre los riesgos de descargar y utilizar aplicaciones de préstamos a través de la red pública de internet

Publicado el 19 Octubre 2021



Comunicado 2452

Derivado de diversas denuncias ciudadanas sobre aplicaciones maliciosas relacionadas con préstamos inmediatos a través de la red pública de Internet, personal de la Unidad de Policía Cibernética de la Secretaría de Seguridad Ciudadana (SSC) de la Ciudad de México, realizó un análisis e identificó al menos 80 apps que no se encuentran debidamente reguladas por la Comisión Nacional para la Protección y la Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

La Policía Cibernética detectó que las denuncias sobre este tema han crecido, aún después de informar anteriormente sobre los riesgos al solicitar dinero por este medio y describió que valiéndose de la necesidad económica de los cibernautas, dichas aplicaciones ofrecen falsos préstamos inmediatos y después, supuestos gestores de cobranza al no detectar el pago puntual, recurren a métodos violentos por medio de acoso, amenaza y extorsión.

A través del patrullaje virtual realizado por el personal de la SSC, se identificaron otras situaciones inusuales, ya que para instalar dichas aplicaciones los usuarios dan acceso a su agenda de contactos y galería de imágenes, que utilizan si la persona no paga en

tiempo y forma, y recibe una serie de amenazas vía telefónica o mediante mensajes de WhatsApp o, en algunos casos, las fotos las pusieron en redes sociales ofreciendo supuestos servicios sexuales o refieren que el afectado es un defraudador.

Tras un análisis se identificó que algunos ciudadanos solo descargaron la aplicación y que nunca solicitaron el préstamo o que nunca les realizaron la transferencia de dinero; sin embargo, sí otorgaron los permisos para acceder a su información personal; ante las denuncias ciudadanas, la SSC a través de la Policía Cibernética gestionó con la autoridad competente para dar de baja dichas aplicaciones con la información recopilada y el reporte de denunciantes.

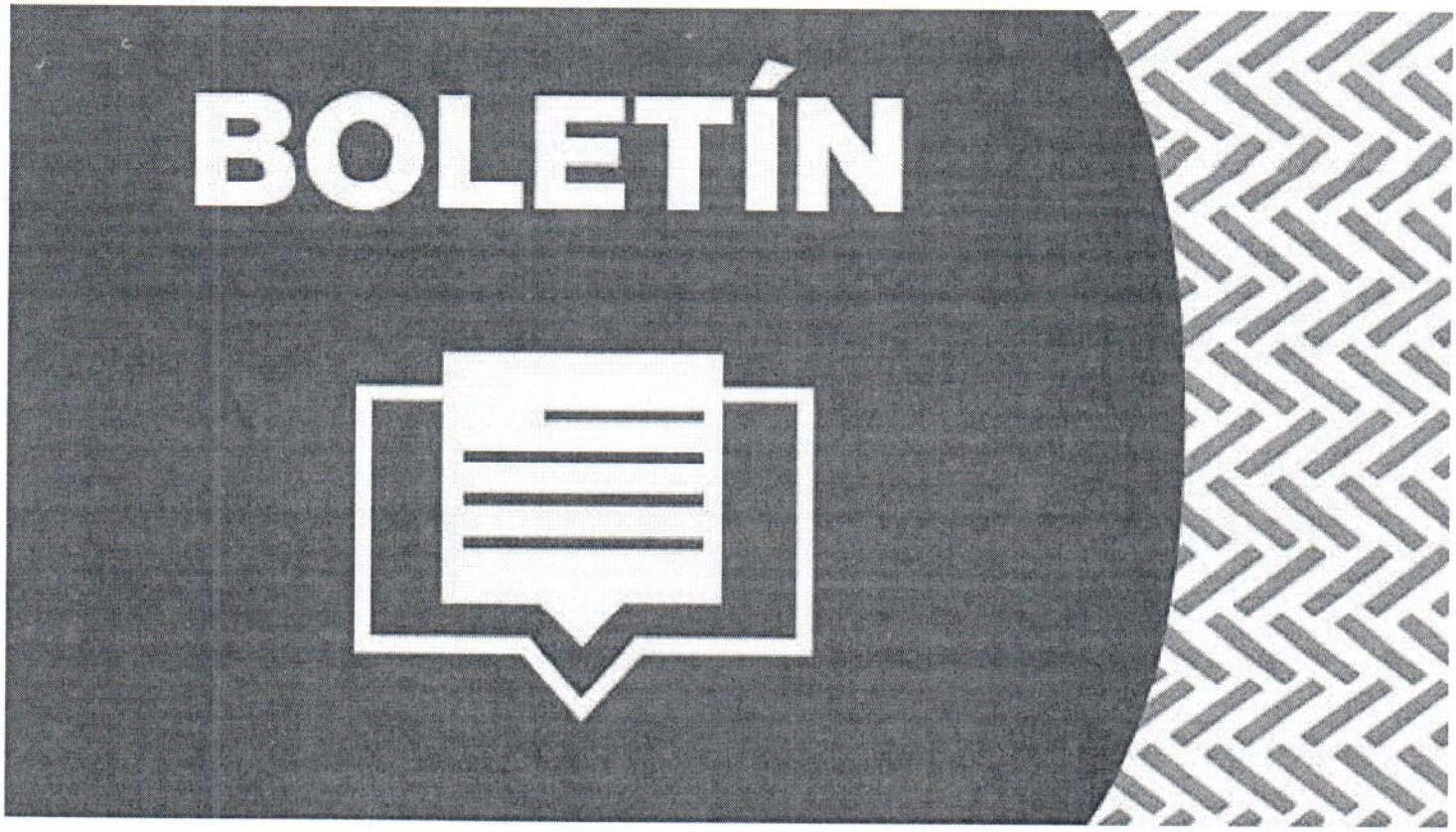
Como resultado del monitoreo las 24 horas del día de la red pública de Internet, la Policía Cibernética alerta a la ciudadanía de este modo de operar y emite recomendaciones a los cibernautas:

• Descargar y actualizar antivirus en todos los dispositivos móviles • Ser precavidos con los permisos que se otorgan cuando se instala una aplicación, revisar términos y condiciones • Verificar que las aplicaciones de préstamos estén reguladas por CONDUSEF https://webapps.condusef.gob.mx/SIPRES/jsp/pub/index.jsp (https://webapps.condusef.gob.mx/SIPRES/jsp/pub/index.jsp) • No confiar en la obtención de préstamos accesibles, con pocos requisitos y sin revisión de buró de crédito • Cuidado al compartir identificaciones o documentos oficiales, podrían ser víctimas de robo de identidad. • Verificar el domicilio físico de la empresa y realizar llamadas telefónicas para conocer las condiciones crediticias. • Evitar llenar formularios con datos personales, números de cuentas o tarjetas bancarias, sobre todo si son en ventanas emergentes • No proporcionar ningún tipo de anticipo económico a través de transferencias o depósitos a cuentas de terceras personas o intermediarios

Para cualquier duda u orientación, así como en caso de detectar eventos sospechosos en el ciberespacio, la Policía Cibernética de la SSC, pone a disposición de la ciudadanía el número telefónico 55 5242 5100 ext. 5086, el correo electrónico policia.cibernetica@ssc.cdmx.gob.mx o las cuentas de redes sociales oficiales @SSC_CDMX y @UCS_GCDMX.

177: La Policía Cibernética de la SSC alerta a la ciudadanía sobre los riesgos de descargar aplicaciones y ceder permisos para acceder a información personal

Publicado el 18 Enero 2022



Comunicado 177

La Unidad de Policía Cibernética de la Secretaría de Seguridad Ciudadana (SSC) de la Ciudad de México, alerta a la ciudadanía sobre mensajes que se reciben vía mensajería instantánea con imágenes con contenido inapropiado y textos en los que argumentan que las personas que aparecen en las fotografías, son deudores de préstamos o que cometieron algún ilícito.

Dichos mensajes son enviados por los cibercriminales quienes lograron obtener información de sus víctimas debido a que ellas o sus contactos, descargaron aplicaciones de préstamos y cedieron los permisos para acceder a información sensible de su dispositivo móvil.

De acuerdo la Policía Cibernética de la SSC y sus patrullajes constantes en la web, la práctica de exponer documentación personal de otros sin su consentimiento con la finalidad de acosar, amenazar o vengarse en línea, se le considera como Doxing.

A través de los monitoreos constantes en el red pública de Internet, la Policía Cibernética encontró que una vez obtenida la información, los cibercriminales comienzan a intimidar, extorsionar e incluso amenazar a sus víctimas, diciéndoles que

serán expuestos en redes sociales o en sitios para adultos donde adjuntarán fotografías privadas e incluso mencionan que embargarán sus bienes materiales.

Esta Secretaría pide a los internautas y usuarios tener mucha precaución, ya que cuando se descargan aplicaciones sin conocer sus políticas de uso, podría resultar muy peligroso, ya que además de proporcionar datos generales como domicilio, lugar de trabajo o el número de teléfono personal, los cibercriminales también pueden acceder a información confidencial, lo que podría perjudicar la integridad física y psicológica de la o las personas afectadas.

Una constante entre las víctimas que han denunciado a la Unidad de Policía Cibernética es que, una vez que su información privada fue expuesta, además del daño tecnológico, sufren ataques de pánico, ansiedad o paranoia, por ello, la SSC emite las siguientes recomendaciones:

• El hecho de que una aplicación se encuentre en el catálogo de una tienda de aplicaciones no significa que sean auténticas.

• Antes de descargar una aplicación verifica su calificación, así como los comentarios de los usuarios.

• Evita almacenar contenido multimedia de documentos, tarjetas bancarias o íntimo.

• Recuerda que los dispositivos móviles siempre pueden estar en riesgo y con ello tu información.

• Procurar acudir a instituciones financieras para cualquier solicitud de préstamo y corrobora su existencia ante la CONDUSEF.

• Recuerda instalar y mantener actualizado un antivirus en tus dispositivos móviles y ordenadores lo que te ayudará a detectar cualquier anomalía.

• Evita ingresar credenciales o datos bancarios a un sitio web no verificado o mandarlos mediante mensajería instantánea, pues pueden ser utilizados por terceros.

• No te dejes engañar por promociones excesivas, servicios gratuitos o tasas de interés muy bajas, podrías estar expuesto a un engaño.

• Restringe, bloquea y elimina todo medio de contacto con los agresores, evita acceder a intimidaciones y amenazas.

• Evita contestar llamadas o mensajes de números desconocidos y, en caso de hacerlo, no proporciones datos personales o bancarios, asimismo verifica y reporta de inmediato ante las autoridades.

• Nadie esta exento de ser víctima de algún delito a través de Internet, por ello debemos habituarnos a protegernos en el mundo virtual tanto como en el físico.

Ante cualquier duda, consulta a los expertos, la Unidad de Policía Cibernética se encuentra en atención a la ciudadanía las 24 horas de día a través del número telefónico 55 5242 5100 ext. 5086, del correo electrónico policia.cibernetica@ssc.cdmx.gob.mx o las cuentas de redes sociales oficiales @SSC_CDMX y @UCS_GCDMX.