LAS NOTICIAS
Fecha: 09/10/2024 Audiencia: 12.000 Sección: LOCAL
Vpe: $1.240.002 Tirada: 3.600 Frecuencia: DIARIO
Vpe pág: $1.370.325 Difusión: 3.600
Vpe portada: $1.370.325 Ocupación: 90,49%

“Me están amenazando a mí y a mi familia”: la guerra que lleva SERNAC contra las apps de préstamos que extorsionan a usuarios

La investigación del ente fiscalizador determinó que la mayoría de estas empresas no existen formalmente o funcionan bajo una fachada dudosa.

Los casos con indicios de delitos fueron derivados a PDI y además SERNAC ofició a Google y Apple para evitar la proliferación de estas aplicaciones.

En algunos casos, se solicitan datos mínimos a las personas, incluso sólo su cédula de identidad, y supuestamente se otorgan créditos que van desde los $10 mil hasta $1 millón.

El Servicio Nacional del Consumidor (SERNAC) ha estado investigando una serie de aplicaciones móviles presentes en las tiendas de Google y Apple, que estarían operando dentro del marco regulatorio nacional en el otorgamiento de créditos.

El método operativo suele ser repetitivo: se desarrolla una aplicación móvil, se publica en la tienda de aplicaciones correspondiente y, de esta manera, se comienza a ofrecer microcréditos de forma “fácil”.

Para ello, la app solicita al usuario ingresar ciertos datos mínimos para su evaluación crediticia, como, en algunos casos, sólo la cédula de identidad. Luego de este proceso, se puede supuestamente acceder a créditos que van desde los $10.000 hasta $1.000.000.

Hasta aquí, la propuesta parece atractiva. ¿El problema? La mayoría de estas empresas no existen formalmente o funcionan bajo una fachada dudosa, con domicilios que no se pueden verificar o que se encuentran fuera del país.

Además, el verdadero riesgo aparece después de instalar la aplicación: la mayoría de estas apps requieren que el usuario otorgue permisos que prácticamente entregan el control total del teléfono al prestamista. El nivel de información al que acceden es muy amplio, incluyendo la agenda de contactos, registro de llamadas, SMS, ubicación, correos electrónicos, uso de la cámara y teléfono, acceso al IMEI, alarmas y notificaciones invasivas, entre otros. Se trata de datos personales y, en algunos casos, incluso de información sensible.

La implicancia de este conjunto de permisos se manifiesta después de que se otorga el crédito: cobranza extrajudicial de manera abusiva. Los usuarios reportan experiencias como alarmas autoprogramadas en sus teléfonos, bloqueo de su uso, mensajes emergentes imposibles de eliminar y contacto telefónico con terceros. Estas prácticas se suman a otros métodos de cobranza abusivos e ilegales, como llamadas de amenaza o intentos de extorsión mediante contacto directo con los usuarios.

“Me han llamado y enviado mensajes a través de redes sociales insistentemente, incluso utilizando amenazas telefónicas en que ponen en riesgo mi vida y la de mis hijos. “reporta una de las usuarias que descargó Mint Mate.

Otra persona que reclamó en SERNAC, plantea: “Estoy recibiendo correos electrónicos de amenaza y extorsión por parte de una aplicación de préstamos llamada: IPréstamos de play store, desde hace 1 semana; me están cobrando un supuesto préstamos el cual no he solicitado; y me amenazan con difundir que soy estafadora por redes sociales”.

La App Crédito Claro también concentra reclamos, uno de ellos plasma que:” En una ocasión pedí un préstamo en esta aplicación, pagué y me cargaron automáticamente como 3 créditos los que no he pagado porque me están cobrando aproximadamente el triple por los intereses y me están amenazando a mí y a mi familia, que si no pago me harán daño, les dije que les devuelvo lo que me cargaron pero insisten en que debo pagar intereses, pero yo no pedí este dinero. Cambié mi número telefónico y empezaron a llamar a mi familia.

De la misma App, esta vez el reclamo obtenido del store de Google, indica que “Me atrasé 1 día en pagar la cuota y comenzaron con llamadas y mensajes cobrándome de una manera enfermiza, incluso me llegó un mensaje amenazando de muerte y que mis

órganos valdrían más que la cuota que les debía”.

EzPeso también es otra de las Apps bajo la mira, un usuario reclamó en SERNAC lo siguiente: “Ahora hace tan solo unos minutos me habló un nuevo número que está publicando mi foto y me envió más de 100 veces el mismo mensaje, por favor les pido su ayuda con estos estafadores.”

Es la serie de antecedentes recabados, es que el SERNAC culminó oficiando a Google y Apple para que se pueda evaluar la eliminación de las apps que no cumplan con los requisitos mínimos tanto de la ley del consumidor o de otras leyes vigentes, además, de que las stores puedan revisar las apps que, habiéndose eliminado de las tiendas, siguen instaladas en los teléfonos móviles de los usuarios. Por último, se requerirá a ambas empre-

Continúa en la página siguiente...

Fecha: 09/10/2024 Audiencia: 12.000 Sección: LOCAL
Vpe: $556.709 Tirada: 3.600 Frecuencia: DIARIO
Vpe pág: $1.370.325 Difusión: 3.600
Vpe portada: $1.370.325 Ocupación: 40,63%

Viene de la página anterior...

sas el trabajo en conjunto para evitar el avance de apps de índole fraudulenta en nuestro país.

Respecto a posibles delitos asociados tras las aplicaciones publicadas o que alguna vez lo estuvieron, pero pueden seguir operando, el Servicio ha derivado todos los antecedentes a la Policía de Investigaciones (PDI) para que puedan pesquisar los orígenes de éstas y realizar todas las diligencias que correspondan.

LAS APLICACIONES BAJO LA MIRA:

De las aplicaciones indagadas, 12 ya han sido eliminadas de los stores, se tratan de: "DiviCrédito", "Online Finanzas", "Nuevo CLP-Préstamo personal", "FlexiCuota-Préstamo", "FácilCuota-Préstamo", "TiFi Moni - Línea de Crédito", "CuotaPlazo Cred-Préstamos", "CrediYa - móvil personal", "Súper Préstamo -Online Crédito", "Bogofin - Préstamos en Línea", "Tu Plata - Préstamo de Crédito" y "Creditolibre Préstamo en Línea".

En este caso, el Sernac ha derivado los antecedentes a la Policía de Investigaciones por eventuales delitos de amenazas, prácticas coercitivas y hostigamiento, además de la información que solicitarán a las Stores para ver cantidad de posibles usuarios que aún tengan instalada dichas aplicaciones a pesar de haber sido eliminadas de las tiendas.

Por otra parte, existen 14 aplicaciones que siguen vigentes, particularmente disponibles en la store de Google, han sido derivadas a PDI por contener reclamos por "amenazas", "hostigamiento", entre otros eventuales delitos, son:"i-Préstamos: Rápido Crédito", "CashFácil: Préstamo en línea", "CreditoClaro - Préstamo Rápido", "ALFA - Préstamos Personales", "Dinero expreso-Préstamo fácil", "SimpleCash-Préstamo", "CreditoJusto - Préstamo Rápido", "Autobús Efectivo", "PresTay: Crédito en Línea", "Prestela: Credito y Prestamos", "FlashPeso", "CredMax - seguro y rápido", "ECLIP-Crédito Premium y Seguro", "Fincash - Préstamo rápido".

Así, se totalizan 26 aplicaciones vigentes o no vigentes que han sido derivadas por eventuales delitos.

En el caso de la store de Apple, las aplicaciones indagadas por eventuales delitos, son: "OneWay Prestamos" y "CréditoFácil".

Por último, otro grupo de 5 aplicaciones serán solicitadas para revisión en la store de Google por utilización y petición de datos particulares sin necesariamente un otorgamiento de préstamo, o casos en los que se deposita automáticamente un préstamo sin haberlo solicitado, son: "Expertos en préstamos", "MintMate-Préstamo en Efectivo", "PrestaBien Pro, Crédito", "SerCrédito" y "Tirofacil - Préstamo",

Mientras estas irregularidades se subsanan junto a las stores, y los antecedentes son procesados por PDI, el SERNAC hace un llamado explícito a no utilizar apps de créditos como las mencionadas anteriormente y a siempre acudir a las instituciones financieras acreditadas por la Comisión para el Mercado Financiero (CMF) para el otorgamiento de créditos de consumo.

¿QUÉ TIPO DE PERMISOS SE OTORGAN A UNA APLICACIÓN?

Cuando una persona descarga una aplicación en su teléfono móvil, tiene que permitir o rechazar diversos permisos para que ésta acceda a información personal. Por esta razón, es fundamental tener cuidado con los permisos que se le otorgan, ya que algunos pueden poner en riesgo tu privacidad, e incluso, tu seguridad.

Alguno de los permisos a los que las y los usuarios deben prestar más atención son:

- Cámara: Una aplicación fraudulenta podría activar la cámara en secreto y grabar sin el consentimiento del usuario.
- Contactos: Aplicaciones maliciosas pueden enviar mensajes o realizar llamadas a los contactos para propagar spam o estafas.
- Teléfono: Las apps pueden registrar hábitos y realizar llamadas sin el consentimiento de las personas.
- Almacenamiento: Aplicaciones malintencionadas pueden leer, modificar o eliminar los archivos personales que están en el dispositivo.

De todas formas, en teléfonos que tengan sistema operativo Android, se pueden verificar los permisos de las aplicaciones, a través de Google Play o la misma configuración del teléfono.

Es importante revisar estos permisos periódicamente para garantizar la seguridad de las y los usuarios en sus dispositivos móviles y no ser objeto de eventuales delitos.