



Saltillo, Coahuila de Zaragoza; a día 22 de agosto del 2024
Oficio No. SSP/UT/661/2024

Luis Ríos:

Me refiero a su solicitud de información realizada a esta Dependencia a través del Sistema de solicitudes de acceso a la información: SISAI 2.0, misma que quedó registrada bajo el número de folio **050094500018524** en la que insta lo siguiente:

"Solicito se me entregue un informe respecto de los hallazgos que se han reportado desde la unidad de Policía Cibernética a raíz de solicitudes para investigación o patrullajes virtuales. Solicito se me informe las prácticas que han sido identificadas y que pueden acreditar delitos durante los años 2019, 2020, 2021, 2022, 2023 y 2024. Además, solicito que se me informe cuántos de estos operativos o acciones fueron insumos para el inicio de una carpeta de investigación en Coahuila, y cuántas de ellas están judicializadas." ... (SIC)

En mérito de lo anterior, de conformidad con los artículos 99 y 102 de la Ley de Acceso a la Información Pública para el Estado de Coahuila, se le comunica lo conducente:

PRIMERO. – Respecto a "Solicito se me entregue un informe respecto de los hallazgos que se han reportado desde la unidad de Policía Cibernética a raíz de solicitudes para investigación o patrullajes virtuales".

HALLAZGOS

Actividades Sospechosas en Redes Sociales.

- Suplantación de Identidad para fraudes: Identificación de 128 perfiles falsos en Facebook utilizados para realizar fraudes mediante la venta o promoción de productos y servicios
- Suplantación de identidad de empresas de turismo: Se han identificado 21 páginas de Facebook y 5 páginas webs apócrifas, suplantando la identidad de Agencias de Turismo y Cadenas Hoteleras
- Perfiles falsos dedicados a la extorsión sexual: Se identificaron 41 perfiles falsos utilizando imágenes de modelos, los cuales operaban en la red social de Instagram, contactando principalmente a hombres con el fin de establecer un vínculo amoroso para posteriormente obtener videos sexuales íntimos a través de videollamadas y de esta forma extorsionarlos con enviarlos a su familia
- Robo de artículos a través de Marketplace de Facebook: Se identifica que otra modalidad de fraude a través de Facebook se centra principalmente en usuarios que venden artículos como Computadoras, Celulares, Videojuegos, Smart TV.
- Publicidad de Aplicaciones Monta deudas: Se han identificado un aproximado de 95 aplicaciones monta deudas, tomando en cuenta que frecuentemente cambian su nombre para no ser identificadas
- Se identificaron 10 páginas apócrifas del gobierno Federal, para tramites de pasaporte, visa, apoyos sociales
- Venta de drogas a través de redes sociales: Se tiene en investigación 6 perfiles de Instagram que, mediante historias publicadas, promocionaba la venta de artículos con sustancias estupefacientes
- Publicación de venta de armas en grupos locales: identificación y eliminación de 15 publicaciones en grupos de ventas de armas de fuego que infringían las normas comunitarias de Facebook



- Páginas de Facebook de servicios esotéricos: Se han identificado 15 páginas dedicadas a extorsionar mediante la promoción de servicios esotéricos.
- Grupos de venta de contenido íntimo sexual: 4 Grupos de TELEGRAM dedicados a vender contenido sin autorización de menores y mayores de edad
- Plataforma web dedicada a los servicios sexuales que se dedica a extorsionar a las personas que soliciten información.
- Números telefónicos cuyo objetivo es extorsionar: Se identificaron 495
- Correos electrónicos con phishing: 15 correos electrónico suplantando la identidad de Microsoft

SEGUNDO. - Referente a "Solicito se me informe las prácticas que han sido identificadas y que pueden acreditar delitos durante los años 2019, 2020, 2021, 2022, 2023 y 2024"

PRACTICAS DELICTIVAS IDENTIFICABLES

| | | |
|------|---------------------------|--|
| 2020 | Phishing | Se identifica un aumento de phishing relacionado con ayudas gubernamentales y compras en línea debido a la pandemia de COVID-19. |
| | Fraude | Transacciones fraudulentas en plataformas de comercio electrónico y servicios en línea. |
| | Extorsión telefónica | Extorsión mediante llamada telefónica, mencionando pertenecer a algún cartel |
| | Suplantación de identidad | Creación de perfiles falsos en redes sociales para realizar extorsiones, fraudes y difamación de identidad |
| | | |

| | | |
|------|---------------------------|--|
| 2021 | Phishing | Creación de sitios web fraudulentos imitando entidades financieras para engañar a los usuarios. |
| | Fraude | Fraudes asociados a la venta de productos y servicios inexistentes a través de redes sociales. |
| | Extorsión telefónica | Amenazas de acudir a domicilio si no se deposita una cantidad |
| | Suplantación de identidad | Uso de identidades robadas para acceder a servicios financieros y realizar transacciones fraudulentas. |
| | Monta deudas | Uso de tácticas de acoso y amenazas a través de las aplicaciones para obtener pagos. |



| | | |
|------|---------------------------|--|
| 2022 | Phishing | Uso de mensajes SMS y aplicaciones de mensajería instantánea para distribuir enlaces maliciosos. |
| | Fraude | Fraudes asociados a la venta de productos y servicios inexistentes (Modalidades: renta de cabañas, venta de electrónicos, robo de consolas, dispositivos electrónicos) |
| | Extorsión telefónica | Amenazas de causar algún daño, mencionando que pertenecen a alguna autoridad o grupo delictivo |
| | Suplantación de identidad | Suplantación de identidad para fraudes laborales y académicos. |
| | Monta deudas | Integración de spyware en las aplicaciones para obtener datos personales de los usuarios. |
| | Hackeo | Aumentan el número de hackeos a Facebook e Instagram para extorsionar, hacer fraude y robar más cuentas |

| | | |
|------|---------------------------|---|
| 2023 | Phishing | Empleo de inteligencia artificial para personalizar mensajes de phishing y aumentar la tasa de éxito. |
| | Fraude | Utilización de redes de votos para ejecutar fraudes automatizados y a gran escala. |
| | Extorsión telefónica | Uso de deepfakes para amenazar a figuras públicas y empresariales. |
| | Suplantación de identidad | Uso de inteligencia artificial para clonar la imagen o voz de servidores públicos |
| | Monta deudas | Publicidad en redes sociales para la instalación de aplicaciones de prestamos |
| | Hackeo | Uso de deepfakes para amenazar a figuras públicas y empresariales. |

| | | |
|------|---------------------------|--|
| 2024 | Phishing | Utilización de deepfakes para suplantar identidades y realizar fraudes más creíbles, a través de correo electrónico, SMS y redes sociales. |
| | Fraude | Fraudes asociados a la venta de productos y servicios inexistentes a través de redes sociales. Modalidades: Créditos, Marketplace, Amoroso, Turismo, Trámites Gubernamentales, inversiones, Soporte Banca Móvil, Subastas |
| | Extorsión telefónica | Amenazas de causar algún daño, mencionando que pertenecen a alguna autoridad o grupo delictivo, Modalidades: Telefónica, Secuestro Virtual, Sexual |
| | Suplantación de identidad | Uso de inteligencia artificial para clonar la imagen o voz de servidores públicos |
| | Monta deudas | Implementación de mecanismos para evadir las políticas de las tiendas de aplicaciones oficiales y continuar operando ilegalmente. |
| | Hackeo | Suplantación de identidad de paqueterías para solicitar código de verificación |



TERCERO. - En relación a "Solicito que se me informe cuántos de estos operativos o acciones fueron insumos para el inicio de una carpeta de investigación en Coahuila, y cuántas de ellas están judicializadas"

R: En atención a este punto me permito informar que, durante el periodo 2023-2024 se encontraron cinco (05) carpetas de investigación en Coahuila.

De conformidad a lo dispuesto por el artículo 100 de la Ley Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, si Usted no está conforme con la presente respuesta, tiene el derecho de hacer valer el recurso de revisión, de acuerdo a lo establecido por el artículo 107 de la misma ley se da por cumplida la solicitud.

Sin otro particular quedo de Usted

**LA TITULAR DE LA UNIDAD DE TRANSPARENCIA
DE LA SECRETARIA DE SEGURIDAD PÚBLICA**

LIC. ERIKA CHAIRES GONZALEZ