Boletín de Fraude 15 de Febrero 2022.

01 Condusef emite alerta sobre empresa de inversiones; afirmaba estar “regulada”.

02 · Adultos mayores, ¿cómo pueden protegerse de los fraudes en línea?.

03 Reino Unido incauta por primera vez archivos NFT, relacionados a caso de fraude fiscal.

04 California, con un récord de 25 millones de dólares en reclamos de estafa de desempleo.

05 Durante enero suplantaron identidad de ocho sofomes y dos sofipos.

06 Cuáles son los ciberfraudes más comunes y cómo protegerte de ellos.

¿HAS SIDO VÍCTIMA DE FRAUDE O AÚN NO LO SABES?

CONTÁCTANOS

protiviti®
Global Business Consulting

Protiviti líder en servicios de consultoría de riesgos de negocios y auditoría interna, apoya a la lucha antifraude.
Quincenalmente distribuimos esta recopilación de las notas más sobresalientes relacionadas con delitos de cuello blanco.

protiviti®
Global Business Consulting

Condusef emite alerta sobre empresa de inversiones; afirmaba estar “regulada”.

- La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) se desmarcó de la empresa Invexia o Estrategias y Servicios Inv. SAPI de CV, la cual ofrece esquemas de inversión y aseguraba estar regulada por las autoridades financieras de este país.

07 febrero 2022

El Economista.

En su cuenta de Twitter, la Condusef indicó que Invexia no es una empresa regulada por esta autoridad, por lo que sugiere al público general ahorrar e invertir en instituciones formales. "Invexia o Estrategias y Servicios INV, SAPI de CV, no es una empresa regulada por la Condusef. ¡Protege tu dinero!, ahorra e invierte en instituciones formales", explicó el organismo a cargo de Óscar Rosado Jiménez.

De acuerdo con fuentes enteradas de la situación, Invexia aseguraba estar regulada por las autoridades financieras del país al ser una Sociedad Anónima Promotora de Inversión de Capital Variable (SAPI); sin embargo, operar bajo dicha figura no implica ser entidad financiera autorizada o regulada tanto por la Condusef como por la CNBV.

"Al ser parte del sistema financiero mexicano, la empresa (Invexia) se encuentra sujeta a la supervisión de la Comisión Nacional Bancaria y de Valores (CNBV), de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), Procuraduría Federal del Consumidor (Profeco) y por la Secretaría de Hacienda y Crédito Público (SHCP)", se leía en la página de Internet de Invexia todavía hace algunos días.

Ante los alertamientos de la autoridad en redes sociales, esta entidad modificó su página de Internet y eliminó cualquier rastro que pudiera dar el entendido de que su modelo está supervisado por la autoridad financiera.

Ahora, en su página, se explica que el modelo de negocio, por el cual genera rentabilidad, se basa en la relación con una sociedad financiera de objeto múltiple (sofom), de la cual no se dice su nombre y sólo se limita a informar que dicha entidad está dedicada al otorgamiento de créditos personales a empleados de dependencias gubernamentales, con descuentos vía nómina.

"No confíes en cualquier empresa que diga estar regulada por la Condusef. Verifica que esté autorizada en el SIPRES (Sistema de Registro de Prestadores de Servicios Financieros)", añadió la Condusef en sus redes sociales.

Esta alerta se suma a la emitida recientemente por la autoridad sobre Xifra Business Group, firma que aseguraba estar regulada por la Condusef y CNBV, respecto a sus esquemas de inversión basados en operaciones con criptomonedas.

Sin embargo, la autoridad indicó que Xifra Business Group no está regulada y su sofom, de nombre Finanzas Que te Acompañan, no tiene el permiso de captar recursos del público en general. Asimismo, la Condusef apuntó que dicha financiera de objeto múltiple ha incumplido con su obligación de validar su información corporativa y de localización, lo que la llevaría a perder el registro ante tal autoridad.

protiviti®
Global Business Consulting

Adultos mayores, ¿cómo pueden protegerse de los fraudes en línea?

13 Febrero 2022

El Financiero.

Los fraudes cibernéticos mediante plataformas digitales aumentaron considerablemente durante la pandemia porque la forma de interactuar, de comprar y socializar creció por temor a contagiarse, afirma Manager de la empresa de ciberseguridad.

El crecimiento y "éxito" de estos crímenes, ya sea vía telefónica, por internet o aplicaciones de mensajería instantánea, se debe a que los delincuentes atacan principalmente las emociones y sentimientos de las víctimas y se hacen pasar por familiares, amigos e incluso jefes o compañeros de trabajo.

"Los adultos mayores son un blanco fácil. Ellos crecieron en una generación donde esas tecnologías no existían y tienen miedo de usarlas. Como mayores han perdido capacidades visuales, auditivas, motoras e incluso de memoria, lo que provoca que les cueste más trabajo usar las nuevas tecnologías", aseguró el especialista en entrevista.

Alfredo Sastré señala que los adultos mayores utilizan las plataformas digitales principalmente para sentirse queridos, atendidos y estar cerca de sus familiares y amigos, por lo que utilizan computadoras y teléfonos inteligentes para acceder a sus correos electrónicos, aplicaciones de mensajería instantánea, leer y mantenerse informados y es ahí cuando pueden ser víctimas de ataques o fraudes cibernéticos.

¿Cómo evitar verse defraudado?

Para Sastré Barraza, las principales herramientas contra los ataques cibernéticos son la prevención y la educación.

Señala que en materia de educación, hay esfuerzos diversos en universidades, organizaciones y empresas están haciendo labor social para incluir a los adultos mayores en la era de la digitalización.

Ejemplos de ellos son los cursos realizados por la plataforma Construyendo y Creciendo, quienes abrieron un aula en la Ciudad de México para compartir conocimiento y ayudar a desarrollar habilidades a los adultos mayores en el manejo de herramientas digitales.

La banca también cuenta con programas de concientización hacia el consumidor, como algunos bancos que tiene una sección específica para adultos mayores. "Creo que como ciudadanos y familiares debemos orientarlos también e invitarlos a acudir a este tipo de alternativas. Hace falta más difusión, ya que esta información no está al alcance de este tipo de personas", afirma.

Sobre la prevención, el especialista en ciberseguridad menciona que es importante tener un antivirus que ayude a detener cualquier tipo de malware que se quiera instalar cuando algún adulto mayor dé clic a una liga de alguna falsa promoción, así como colgar de inmediato cualquier llamada de extorsión.

protiviti®
Global Business Consulting

Adultos mayores, ¿cómo pueden protegerse de los fraudes en línea? (Continuación)

13 Febrero 2022

El Financiero.

"La recomendación de los expertos es que ante una llamada de extorsión o intimidante debemos colgar y cortar la llamada de inmediato. Cuelga. Son llamadas que provienen de personas que probablemente estén en cárceles. Cuelga y busca a tu familiar o a un familiar que te ayuda a corroborar la información que te están proporcionando, pero no des información o datos de cuentas bancarias, ni te apresures a realizar transferencias bancarias", aconseja.

Otros pasos a seguir

- Utilizar contraseñas y controles de acceso de al menos ocho caracteres.
- No exhibir datos personales: fotografías, videos, ubicación en tiempo real, información de familiares o compañeros de trabajo.
- En encuestas, entrevistas o promociones no brindar información sensible.
- Nunca proporcionar número de tarjetas de crédito, bancos, INE, o información médica.
- Ser desconfiado ante ofertas y promociones.
- No dar clics a enlaces emergentes o descargar archivos a tu computadora.
- Los fraudes digitales van a seguir creciendo, afirma Sastré y una manera efectiva de prevenir es mantenerse informado y generar concientización.

"Todos tenemos en nuestras familias alguna persona mayor. Creo que deberíamos de actuar de manera más proactiva con ellos y no solo enfocar nuestros esfuerzos a provocar que se sientan queridos, sino en ayudarlos en hacerlos un poco más conscientes de los riesgos que pueden tener en los canales digitales", añade.

En caso de ser víctima de un fraude o delito cibernético es necesario considerar lo siguiente:

Reporta el perfil en la red social, si la acción no es grave.

Respalda la evidencia digital (mensajes, correos electrónicos, fotos, conversaciones) haciendo capturas de pantalla y copiando las direcciones electrónicas de las páginas web donde se ubique la prueba. En caso necesario presenta la denuncia correspondiente dando seguimiento al caso, en contacto con el Ministerio Público.

Llama al 088, donde la Guardia Nacional brinda orientación para realizar la denuncia ante el Ministerio Público. Guarda el número de folio de atención para darle seguimiento. Demasiado bueno para ser verdad. Los ciberdelincuentes 'venden' ofertas atractivas solicitando un anticipo presumiblemente como apartado; con transferencias electrónicas a cuentas personales a través de tiendas de conveniencia (Oxxo, 7 Eleven); persuadiendo al comprador de seguir negociaciones de adquisición fuera de la plataforma digital; invitando por mensajería instantánea a ingresar a los servicios de la banca en línea solicitando la instalación de aplicaciones o en su defecto el nombre de usuario y contraseña por medio de páginas web apócrifas.

protiviti®
Global Business Consulting

Reino Unido incauta por primera vez archivos NFT, relacionados a caso de fraude fiscal.

Reino Unido ha logrado por primera vez incautar tres archivos en formato NFT, relacionados con un caso de fraude fiscal que usó estos activos para inflar su valor y esconder dinero a las autoridades fiscales.

14 Febrero 2022

El Economista.

NFT, siglas de token no fungible, es una tecnología criptográfica basada en "blockchain" que representa algo único, no sustituible, de forma que garantiza su autenticidad, así como quién es su propietario. Normalmente se compran a cambio de criptomonedas, pero a diferencia de estas no son intercambiables mutuamente, es decir, no son fungibles.

El departamento de Hacienda y Aduanas de Reino Unido (HMRC, por sus siglas en inglés) ha dado a conocer una operación para desarticular una red de 250 empresas falsas que ha conducido en la detención de tres personas por fraude del IVA por valor de 1.4 millones de libras (1.67 millones de euros al cambio).

Como aspecto destacado, es la primera vez que Reino Unido una autoridad del orden es capaz de incautar tres archivos en formato NFT, como ha informado la cadena BBC.

En este caso, HMRC no se ha hecho con el control físico de los tokens digitales, almacenados a través de Blockchain, sino que han emitido una orden judicial que evita que las obras de arte puedan venderse, según ha recogido Sky News.

Reino Unido ya se había hecho previamente con otros criptoactivos diferentes a los NFT, y en todos los casos estos se han puesto a la venta a través de subastas públicas.

protiviti®
Global Business Consulting

California, con un récord de 25 millones de dólares en reclamos de estafa de desempleo.

14 febrero 2022

Milenio.

Una estafa de desempleo operada desde las prisiones de California buscó un récord de 25 millones de dólares del estado y los gobiernos de EU obteniendo más de 5 millones de dólares que se destinaron a vehículos, muebles, bolsos y joyas, dijeron el viernes las autoridades federales.

Los 25 millones de dólares son el botín individual más grande conocido en California, dijo el exfiscal federal McGregor Scott, quien está trabajando con el Departamento de Desarrollo del Empleo del estado para coordinar las investigaciones sobre el fraude.

Sin embargo, la pérdida real de 5 millones de dólares sigue siendo una fracción de los más de 20 mil millones de dólares en beneficios de desempleo que las autoridades creen que han sido robados desde marzo de 2020 cuando el estado aprobó pagos fraudulentos a nombre de los condenados a muerte e incluso de la senadora estadounidense Dianne Feinstein.

Los fraudes fueron operados desde la cárcel y otras partes de California

Los reclusos Daryol Richmond, de 31 años, y Telvin Breaux, de 30, ambos del condado de Los Ángeles, afirmaron falsamente que ellos y otros, incluidos niños menores de edad, habían estado vendiendo ropa o trabajando como personal de mantenimiento, mecánicos u otros trabajos hasta que quedaron desempleados debido a la pandemia de covid-19.

Richmond está encarcelado en la prisión estatal de Kern Valley en Delano, cumpliendo una sentencia de casi 25 años como delincuente reincidente por robo e intento de robo, según los funcionarios penitenciarios.

Breaux se encuentra en la Institución Correccional de California en Tehachapi, cumpliendo 15 años por robo con arma de fuego, entre otros delitos. Usaron teléfonos celulares, correos electrónicos y llamadas telefónicas de contrabando desde la prisión para comunicarse con otras personas fuera de las prisiones, dicen los investigadores.

La nueva acusación los acusa junto con seis residentes del sur de California de conspiración para cometer fraude postal y robo de identidad con agravantes, cargos que conllevan una pena máxima de 20 años en una prisión federal y una multa de 250 mil dólares.

Se alega que crearon cuentas de correo electrónico falsas y utilizaron diferentes direcciones de calles en el sur de California para presentar más de 400 reclamos falsos.

protiviti®
Global Business Consulting

Durante enero suplantaron identidad de ocho sofomes y dos sofipos.

15 febrero 2022

El Economista..

Durante el primer mes del año 10 entidades financieras fueron víctimas de suplantación de identidad, esto con la finalidad de defraudar a las personas que buscan acceder a un crédito, informó la Condusef.

Las afectadas fueron: Maquila Suppliers Financial Corp, Albact, Target Capital, Sofomax, Aceleradora Adrenalina, Altum CP, Financiamos tu Necesidad, Progreso Económico, Ku-Bo Financiero y Sociedad Alternativas Económicas.

Los defraudadores contactan personas vía telefónica o por redes sociales ofreciéndoles créditos inmediatos, con pocos requisitos y mensualidades de montos pequeños, luego piden anticipos de dinero para gestionar el financiamiento, pero cuando las víctimas realizan los depósitos no reciben el crédito y es imposible localizar a los promotores.

protiviti®
Global Business Consulting

Cuáles son los ciberfraudes más comunes y cómo protegerte de ellos.

15 febrero 2022

El Economista..

Durante enero el recibo de Telmex de Carmen llegó de 1,184 pesos cuando normalmente paga 399 pesos, revisó el estado de cuenta y se percató que incluía cargos de 785 pesos por concepto de recargas de tiempo aire, las cuales nunca realizó. Al llamar al Telmex para reclamar, la operadora confirmó que fueron recargas realizadas desde la app de la compañía a tres números diferentes, pidió a Carmen cambiar sus contraseñas, procedió la reclamación y el dinero se reembolsó para los siguientes pagos.

Carmen nunca compartió sus contraseñas ni tenía descargada la app de empresa telefónica, pero si había activado su usuario Mi Telmex y ahí tenía domiciliado el pago del servicio. Después de la llamada con Telmex cambió sus claves, borró las que estaban almacenadas dentro de su computadora y en su cuenta de correo.

Actualmente los 15 esquemas de fraudes cibernéticos más comunes, son malware, que se trata de virus que entran a tus dispositivos después de dar clic a links con información, promociones u ofertas falsas; ataques basados en web; phishing, que son mensajes que llegan a través de correos o redes sociales y buscan que brindes información personal por medio de engaños.

También están los ataques de aplicaciones web; los spam; ataques DDos, que buscan inhabilitar sitios webs; usurpación de identidad; filtración de datos; insider threat, que son amenazas internas dentro de las empresas; Botnet, virus troyanos que atacan varias computadoras; manipulación física, daño, robo y pérdidas; fuga de información, ransomware (secuestro de información), ciber espionaje y criptojacking, según datos de la Asociación de Bancos de México (ABM).

De acuerdo con la ABM, los ataques impulsados por motivaciones financieras están en crecimiento, después de que durante años algunas de estas agresiones cibernéticas eran por cuestiones derivadas de activismo.

Para este año se pronostica que seguirán las ciber extorsiones basadas en el cifrado de información, es decir ransomware, que se refiere al secuestro de datos. También habrá incrementos de ataques de phishing, mensajes falsos; vishing, llamadas engañosas donde buscan sacarte información e ingeniería social aprovechando temas relevantes, como Covid-19, economía, empleos, temas bancarios y comercio electrónico.

¿Cómo evitar ser víctima de fraude financiero?

Todas las personas están expuestas a enfrentar algún tipo de ciberataque. Puede ser robo de identidad y que usen datos personales para tomar créditos a tu nombre; que hackeen tus redes sociales, whatsapps o al dar información de seguridad en supuestas llamadas de los bancos.

En el caso de whatsapps, cuyo robo de estas cuentas está creciendo, se recomienda verificar el número, lo cual se puede realizar accediendo a la parte de ajustes, luego se realiza la verificación en dos pasos y se pone una contraseña de protección.

protiviti®
Global Business Consulting

Cuáles son los ciberfraudes más comunes y cómo protegerte de ellos. (Continuación)

15 febrero 2022

El Economista.

Existen una serie de recomendaciones que la Condusef realiza para, en la medida posible, evitar caer en fraudes cibernéticos, por ejemplo, tener cuidado al navegar en la red y no dar clic a páginas sospechosas y siempre verificar que las plataformas tengan el protocolo de seguridad “htpps// y un candado cerrado en la barra de direcciones.

Además, el órgano de verificación recomienda proteger las contraseñas, renovarlas cada cierto tiempo y no almacenarlas en dispositivos.

También se aconseja buscar algún software de seguridad para el celular, tablet o computadora. Sobre la correspondencia que llega a casa, ya sean recibos, paquetes, etc., es importante darle la importancia que se merece, por ejemplo al deshacerse de ella, siempre elimina la parte donde aparezca información personal.

Otro punto relevante para cerciorarte que no eres víctima de fraude, es revisar tu historial crediticio por lo menos una vez al año y verificar que no haya créditos que tú no solicitaste.