Boletín de Fraude 30 de Noviembre 2020

01 **ABM lanza campaña para evitar fraudes bancarios.**

02 **Identifique los diferentes tipos de ciberestafas y evite ser víctima de éstas.**

03 **Por desempleo, ven riesgo de lavado de dinero.**

04 **Conozca y protéjase del SIM Swapping, un fraude que está latente.**

05 **Ghimob, el virus que roba información y comete fraudes con apps de bancos.**

06 **Advierten sobre aumento de casos de phishing.**

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

CONTÁCTANOS

protiviti®

Face the Future with Confidence

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®
Face the Future with Confidence

ABM lanza campaña para evitar fraudes bancarios.

18 noviembre 2020

El Financiero.

La banca reconoció que hay una "ocurrencia desafortunada de fraudes telefónicos y de otro tipo de defraudaciones", particularmente en el entorno digital y cibernético que han afectado a sus clientes, por lo que puso en marcha una campaña masiva para promover acciones con el objetivo de evitar ser engañados por la delincuencia.

El presidente de la Asociación de Bancos de México (ABM), explicó que la campaña "Protégete que no te engañen", es una campaña gremial de todas las instituciones y todos los asociados de la ABM, que inició el 9 de noviembre, precisamente el día del Buen Fin, con una inversión de tres millones de pesos.

"La idea es orientar a los clientes para que puedan prevenir fraudes en llamadas, en mensajes, por correos electrónicos, en todo lo que representa la posible suplantación de identidad o a través de engaños".

Adicionalmente, para prevenir el fraude telefónico piden a sus clientes estén alertas porque la llamada que pretende ser del banco puede que no lo sea.

En el periodo enero-septiembre indicó los reportes de fraudes que tienen vía la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) es que se registraron reclamaciones totales de 8.6 millones por un monto total de 25 mil 300 millones de pesos.

De esos 8.6 millones de reclamaciones, el 61 por ciento se ha resuelto a favor de los clientes, el 22 por ciento se ha resuelto a favor del banco, y el 17 por ciento todavía está pendiente.

De los montos, 34 por ciento se ha resuelto a favor de los clientes y 44 por ciento se ha determinado que son improcedentes, que es a favor del banco. Pendientes queda un 22 por ciento.

Por ello, afirmó en número de reclamaciones y en monto los bancos si han dado respuesta a sus clientes "no sólo rápida, sino efectiva determinando a quien asiste la razón, por consiguiente, debemos de pasar a medir qué representa esto, 8.6 millones en número de reclamos representa el 0.3 por ciento del total de transacciones que hacemos en la banca todos los días. Esto es que ni siquiera llega a la mitad del 1 por ciento".

"La banca sí trabaja para resolver los problemas que tienen los clientes", afirmó.

BOLETÍN DE FRAUDE.

protiviti®
Face the Future with Confidence

Identifique los diferentes tipos de ciberestafas y evite ser víctima de éstas.

18 noviembre 2020

El Economista.

"Amigos!!! Andan llamando de este número (5547423173) para hacer fraude pidiendo datos con el argumento que tengo puntos por vencer", así lo escribió un usuario de Twitter el 13 de noviembre a fin de alertar tanto a la entidad financiera que sigue al arroba, como a otros usuarios, sobre los fraudes que se comenten.

Mientras que otro usuario también denunció en la misma red social sobre los intentos hechos por delincuentes para robar sus datos personales. "Segunda vez que intentan meterme un fraude por teléfono, ya que Uds. no me devolvieron mi dinero, mínimo vayan detrás de ellos, marcan desde este número 55 2232 9359 hace cinco minutos ".

En los últimos meses, este tipo de ciberdelitos aumentaron exponencialmente a raíz del confinamiento por la contingencia sanitaria; este dato no se limita a fraudes telefónicos, también a través de redes sociales o correos.

Ante tantos tipos de fraudes, con características y modos de ataques diferentes, especialistas en ciberseguridad destacan la importancia de que los usuarios aprendan a identificar cómo trabajan los delincuentes y evitar caer en estas estafas.

El director de ciberseguridad en importante financiera, resaltó la importancia de conocer e identificar un ciberdelito.

"A medida que avanza la tecnología y el llamado Internet de las cosas, los dispositivos inteligentes ganan más popularidad, y por supuesto que los ciberdelincuentes disfrutan de una superficie de ataque mucho más amplia, la exposición que se tiene a un tema de robo de identidad, de fraude o cualquier amenaza cada día es más tangible", advirtió.

Dos de los temas que más preocupan a los individuos son el robo de identidad y el fraude, principalmente por contener información que pone en riesgo el patrimonio construido por años.

También detalló que algunos tipos de fraude son conocidos por la población en general, gracias al tipo de nombres con los que se les denominan; sin embargo, en ocasiones no alcanzan a diferenciar el modus operandi y las diferencias entre cada uno.

A su vez, el analista senior de seguridad de importante empresa de ciberseguridad, indicó que las principales motivaciones de los delitos cibernéticos obedecen principalmente a intereses financieros, si bien en raras ocasiones tienen razones distintas a estas, también pueden ser por cuestiones políticas e incluso personales.

protiviti®
Face the Future with Confidence

Identifique los diferentes tipos de ciberestafas y evite ser víctima de éstas. (Continuación)

18 noviembre 2020

El Economista.

Así atacan

Para el analista, la mayor parte del cibercrimen se divide en dos categorías: los ataques dirigidos a los dispositivos digitales y el uso de éstos para cometer otros ilícitos.

El cibercrimen dirigido a los dispositivos digitales se utiliza con el fin de infectarlos, dañar su funcionamiento o los datos que contienen, lo anterior a través de virus informáticos y otros tipos de malware.

Mientras que la segunda categoría es cuando se usan esos mismos dispositivos o redes para la propagación del software malicioso, información e imágenes ilegales, incluso en algunos casos se llegan a utilizar ambos o varios métodos de estafa al mismo tiempo.

“Son muchos canales por los que se pueden recibir amenazas cibernéticas. Sin duda, el correo electrónico es el medio más común, ya que tiene un vínculo directo con la información privada de las empresas. Sin embargo, las redes sociales también son oportunidades que aprovechan agentes maliciosos para atacar a los más desprevenidos, como sucede en las cadenas de Whatsapp que contienen algún link o archivo para descarga”, puntualizó.

El analista indicó que los ciberdelincuentes también usan las aplicaciones disponibles a través de sitios no oficiales para distribuir virus o solicitar permisos al momento de la instalación para tener acceso a la cámara o al micrófono, descargar otras aplicaciones sin consentimiento previo y mostrar publicidad encima de otros programas.

protiviti®
Face the Future with Confidence

Por desempleo, ven riesgo de lavado de dinero.

23 noviembre 2020

El Universal.

El Grupo de Acción Financiera Internacional (GAFI) advirtió que los niveles de desempleo observados en el mundo como efecto de la crisis económica provocada por la pandemia del Covid-19 pueden aumentar el riesgo de lavado de dinero.

En la reunión de ministros de finanzas y gobernadores de bancos centrales del G20, el presidente del organismo antilavado, Marcus Player, expresó que con un número creciente de personas sin trabajo existe mayor probabilidad de que sean utilizados como mulas para transportar dinero para blanquearlo.

Dijo que la pandemia ha provocado el aumento de delitos financieros, como falsificación de productos médicos, estafas y fraudes, aprovechando los estímulos económicos que han otorgado los gobiernos para enfrentar el impacto de la crisis.

Alertó que las empresas que quebraron pueden ser utilizadas para estos fines, porque los delincuentes se pueden apoderar de ellas o les pueden dar dinero en efectivo para blanquear dinero producto de la delincuencia.

En ese contexto, indicó que el sector inmobiliario, el de la construcción y las pequeñas y medianas empresas, son las que corren mayor peligro de ser usadas para el lavado de dinero.

Para contener las vulnerabilidades por estos delitos, pidió a líderes del G20 mantener la lucha contra el lavado de dinero en un lugar destacado de las agendas.

Señaló que precisamente los estándares del GAFI ayudan a los gobiernos a hacer su trabajo en esta materia; si se implementan las recomendaciones de manera efectiva tendrán un impacto inmediato, afirmó.

Aseguró que sólo unidos se podrá garantizar una recuperación económica sólida y sostenible. Se podrá restaurar la confianza en las economías e integridad del sistema financiero.

“Esto es necesario ahora más que nunca, y sería apropiado, con suerte, para un mundo posterior al Covid-19”, afirmó.

Puntualizó que al analizar el camino a seguir, sobre todo en cómo mejorar la resiliencia de las economías, sigue siendo vital considerar protegernos de los fondos ilícitos.

Advirtió que la delincuencia, el terrorismo y el posterior blanqueo de activos que alimentan nuevos delitos plantea graves riesgos para la recuperación y la estabilidad económica.

Todo esto, agregó, socava la competencia justa, obstaculiza el crecimiento, profundiza la desigualdad y erosiona la confianza en la integridad del sistema financiero mundial.

protiviti®
Face the Future with Confidence

Conozca y protéjase del SIM Swapping, un fraude que está latente.

Es un hecho que durante la pandemia los fraudes telefónicos y por Internet tuvieron un incremento considerable, y por tanto consecuencias negativas hacia aquellas personas que cayeron en los engaños de los defraudadores.

23 noviembre 2020

El Economista.

Incluso, la Asociación de Bancos de México (ABM) reconoció el problema y ha promovido una campaña que busca orientar a sus usuarios a no brindar información que ponga en riesgo su patrimonio, desafortunadamente los ciberdelincuentes han encontrado nuevas formas de operar y realizar sus estafas, por ello es importante que sepa cómo protegerse para no caer en sus engaños.

Recientemente, la Policía Cibernética de la Secretaría de Seguridad Ciudadana de la CDMX alertó sobre una nueva modalidad de fraude denominada SIM Swapping o Duplicación de SIM.

De acuerdo con la dependencia, esta nueva modalidad suplanta la identidad de clientes de instituciones bancarias por medio del número telefónico.

La forma en que opera este fraude consiste en que "el delincuente marca para pedir la cancelación y reposición del SIM, y de esta forma accede a las cuentas bancarias ligadas al dispositivo móvil", alertó la Secretaría de Seguridad Ciudadana(SSC) de la CDMX.

Active las medidas de seguridad

Los ciberdelincuentes han encontrado formas más sofisticadas de incurrir en sus ilícitos, sin embargo también la tecnología ofrece una variedad de servicios y opciones que le permiten proteger sus dispositivos, en este caso su teléfono inteligente, ello con el fin de evitar algún tipo de fraude como la suplantación de identidad o en este caso el SIM Swapping.

La SSC de la Ciudad de México recomienda utilizar en sus aplicaciones de mensajería instantánea, el sistema de verificación en dos pasos, donde recibirá un código por SMS a su número telefónico, con ello reduce la posibilidad de que alguien ajeno a su línea telefónica acceda a sus cuentas.

Otra recomendación para evitar ser víctima de un ciberataque es utilizar el reconocimiento facial o de voz, para ello existen aplicaciones como Google Authenticator o Microsoft Authenticator donde también se utiliza la autenticación de dos pasos.

El básico que los expertos recomiendan a la hora de proteger sus dispositivos móviles es la instalación de antivirus confiables y evitar los softwares piratas, aunque parezca un gasto innecesario, en largo plazo y por la coyuntura actual en la que la utilidad de estos dispositivos sirven para realizar operaciones bancarias, le será de gran utilidad.

Por su parte, la ABM recomienda revisar periódicamente sus aplicaciones bancarias, ello con el propósito de no encontrar algún movimiento no reconocido, y en caso de ser así reportarlo de inmediato con su institución bancaria.

En este sentido, las alertas bancarias por parte de su entidad son unas aliadas que le ayudarán estar al tanto de cualquier movimiento sospechoso.

protiviti®
Face the Future with Confidence

Conozca y protéjase del SIM Swapping, un fraude que está latente. (Continuación)

Los expertos también aconsejan que de ser posible solicite a su compañía telefónica el reforzamiento de las medidas de seguridad al momento de realizar operaciones a su nombre.

23 noviembre 2020

El Economista.

Troyanos bancarios, otro peligro

Para importante compañía de seguridad informática, otro método utilizado por los hackers son los llamados troyanos bancarios, los cuales se especializan en proporcionar una ruta directa a las cuentas de otros usuarios.

“Muchos pueden cubrir la interfaz de la aplicación bancaria por sí mismos, simulando que el usuario está introduciendo datos en la aplicación bancaria cuando, en realidad, se los está dando al troyano, que registra la información y la introduce en el portal bancario para que el usuario no sospeche”, advirtió.

Para protegerse de estos troyanos, la compañía recomienda descargar aplicaciones de tiendas oficiales, actualizar constantemente dichas apps, así como bloquear en los ajustes del dispositivo la instalación de software de terceros.

“No te olvides de instalar las actualizaciones de aplicaciones y de sistema, ya que parchean las vulnerabilidades que pueden explotar los cibercriminales”, enfatizó.

No lo tome a la ligera

Proteger su equipo es de gran importancia debido a los riesgos que han ido en aumento, y que de acuerdo con Kaspersky, para el 2021 el panorama en América Latina se vislumbra en una diversificación de ataques dirigidos a los sistemas financieros por grupos cibercriminales locales.

“Lo que más nos preocupa es que en el mercado habrá más ofertas de contratistas para diseñar y lanzar ataques. Es decir, una especie de tercerización de servicios cibercriminales para atacar los bancos y otras instituciones financieras”, detalló.

protiviti®
Face the Future with Confidence

Ghimob, el virus que roba información y comete fraudes con apps de bancos

¡Los ciberataques no paran! Importante empresa de ciberseguridad alertó la reciente actividad de Ghimob, un virus que engaña a sus víctimas a través de un correo electrónico y les instala un archivo malicioso, con el que roban información bancaria y de inversiones.

24 noviembre 2020

Milenio.

Se trata de un archivo que entra como troyano, es decir, que se hace pasar por un archivo fidedigno, que instala un malware, aplicación o software malicioso, para controlar el dispositivo a distancia y cometer robos y fraudes.

Esta alerta se une a la emitida hace poco tiempo por una empresa de ciberseguridad, que avisó sobre la creciente presencia de un igualmente malware llamado Jupyter, que tiene la capacidad de actualizarse para continuar en los sistemas pese a ser detectado por un antivirus para continuar robando información, o bien, utilizando el dispositivo de forma remota.

¿Cómo funciona Ghimob?

Todo comienza cuando sus víctimas reciben un correo electrónico donde les afirman que tienen deudas por saldar y ofrecen más información en un enlace, que al seleccionarlo, aloja el archivo malicioso en el dispositivo.

El malware instalado obtiene la información del dispositivo, así como las aplicaciones que tiene instaladas y logra guardar la contraseña para desbloquear la pantalla, esto lo envía a su servidor, quien tiene a disposición tanto el control del dispositivo como la información del afectado.

Por medio del control remoto, el malware desbloquea la pantalla del dispositivo y lo comienzan a operar.

Ghimob es capaz de espiar 153 aplicaciones de bancos, fintechs, inversión y criptomonedas, y opera principalmente en América Latina, pero también en otras partes del mundo.

Advierten sobre aumento de casos de phishing.

26 noviembre 2020

El Economista.

Durante las últimas semanas aumentó 9% la actividad fraudulenta previo a las ventas del Black Friday, alertó empresa de ciberseguridad.

En un comunicado, la compañía indicó que del 29 de octubre al 18 de noviembre, detectó 196 ataques de phishing por minuto en América Latina ya que esta es la táctica más utilizada para robar las credenciales de las víctimas al momento de que éstas acceden a servicios en línea como comercio electrónico.

Destacó que aunque las promociones del Black Friday comienzan unas semanas antes, este año y debido a las afectaciones por la pandemia del Covid-19, muchas tiendas extendieron sus ofertas durante noviembre; por ende, los ciberdelitos podrían aumentar.

Analista senior del Equipo de Investigación y Análisis en empresa de ciberseguridad, indicó que se bloquearon 5 millones 936,074 intentos de acceder a sitios de phishing en América Latina durante el periodo señalado.