protiviti®
Face the Future with Confidence

Boletín de Fraude
15 de Junio 2019

Protiviti líder en servicios de consultoría de riesgos de negocios y auditoría interna, apoya a la lucha antifraude.

Quincenalmente distribuimos esta recopilación de las noticias más sobresalientes relacionadas con delitos de cuello blanco.

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

CONTÁCTANOS

BOLETÍN
Junio 2019

01 de junio
Formjacking la actividad más lucrativa en 2018.

04 de junio
¿Cuál es el blanco principal de los hackers en México?

10 de junio
Baja 48% suplantación de identidad en bienes raíces de Nuevo León.

11 de junio
Advierten de agencias de viajes “fantasmas”.

11 de junio
Detienen a individuo por cometer fraude al interior del Metro.

12 de junio
Lanzan protocolo para la protección de cuentas bancarias.

14 de junio
Yalitza Aparicio advierte fraude en reventa de boletos para la Guelaguetza.

15 de junio
Hackers usan Google Calendar para promover ofertas fraudulentas.

15 de junio
¿Qué es el código CVV o CVC de tu tarjeta de crédito?

01 de junio

El Universal.

Formjacking la actividad más lucrativa en 2018.

El formjacking es una modalidad de ataque en la que los delincuentes secuestran los sitios web donde compran los usuarios, actividad que se ha convertido en una de las prácticas ilegales más lucrativas para los hackers.

De acuerdo con informes de compañías de seguros, un promedio de cuatro mil ochocientos sitios fue atacados por medio de formjacking en 2018.

"Este ataque representa una entrada de dinero muy rápida. Por cada 10 datos de un sitio web comprometido se pueden obtener unos 45 dólares. Promediando esa información los hackers pudieron haber obtenido ganancias de dos millones de dólares al mes".

En esta práctica los hackers roban información de tarjetas de crédito y de los formularios de pago en los sitios de comercio electrónico. Con los datos obtenidos, realizan fraudes con las tarjetas o venden la información a otros delincuentes en la dark web.

Las aseguradoras destacan que solo en esos ataques que afectaron a portales de venta de viajes, los cibercriminales obtuvieron ganancias por más de 17 millones de dólares. Otras empresas afectadas fueron las dedicadas a ventas de boletos para espectáculos. Los ciberdelincuentes solo tuvieron que inyectar un código malicioso en su objetivo para manipular a donde iba la información bancaria.

Durante el Cyber Defense Cloud Forum, se alertó que esta amenaza tuvo un pico de actividad de un millón de registros en noviembre y diciembre de 2018, los meses con el mayor número de compras en línea. Y se estima que este año seguirá creciendo.

Según los especialistas, entre los consejos más importantes para evitar ser víctima de este tipo de ataques están: tener siempre el control de los navegadores; contar con los parches de seguridad instalados; y tener cuidado con los sitios que usan JavaScript.

04 de junio

El Financiero.

¿Cuál es el blanco principal de los hackers en México?

En los últimos doce meses todas las instituciones del sistema financiero mexicano reconocieron que reportaron incidentes de ciberseguridad, esto a diferencia del año pasado que se negaban a admitir estos sucesos en su contra.

De acuerdo con los resultados preliminares del 'Estado de la Ciberseguridad en el Sistema Financiero Mexicano' realizado por la Organización de los Estados Americanos (OEA), y que será dado a conocer de manera final en las próximas semanas, un total de 240 instituciones financieras que participaron en México, de un universo de 400, reconocieron haber tenido algún incidente de ciberseguridad en el último año. La metodología es similar a la empleada en un estudio anterior realizado por la OEA para la región; México es considerado como un mercado maduro.

El número de personas que conforman los equipos de seguridad digital de una institución financiera es de apenas de 1 a 5 personas, en donde la gran mayoría reportan que sufren algún tipo de ataque diariamente en busca de vulnerarlos, los cuales son detectados en su mayoría por sus propios sistemas y no por terceros, lo cual consideró la OEA que es un avance muy positivo.

También un punto a favor es que los consejos de administración o directivos reciben de manera directa los reportes de estos ataques que sufren las instituciones financieras, lo que ha derivado en que se canalice un mayor presupuesto para estos temas, explicó Belisario Contreras encargado del tema de ciberseguridad de la OEA, ante especialistas del sector financiero mexicanos reunidos en el encuentro organizado por FIBA y que patrocinaron HSBC y Financial Integrity Network. Sin embargo, el informe preliminar también reconoce que muchos de los ataques son exitosos, principalmente en las instituciones de menor tamaño, quienes son las que terminan siendo vulneradas en alguna área.

En la elaboración del reporte participaron entre otros, 9 bancos de desarrollo, 33 bancos comerciales, 59 intermediarios financieros no bancarios, 98 del sector de ahorro y crédito popular, y 17 Fintech, siendo este último sector tecnológico el más atacado, según el estudio. Clave, la seguridad interna: El preinforme mostró también que, a diferencia de otros países de la región, en México las instituciones financieras sí hacen las denuncias ante autoridades federales por ser víctimas de este delito. En el caso de los bancos, son los que tienen el nivel más alto de reporte con un 69 por ciento, el restante no lo hace.

En el panel también participó Elena Calatayud, asesora de ciberseguridad en la Comisión Nacional Bancaria y de Valores (CNBV), quien recordó que en México ya se tiene un protocolo establecido en el sector financiero para el reporte de estos temas. No obstante, dijo que también hay áreas en las que los bancos deben trabajar más, como el combate a los fraudes internos, ya que ha evolucionado mucho, y hoy no son sólo las vulnerabilidades externas, sino también el tema del personal que ayuda a los delincuentes, por lo que consideró que no hay "tecnología segura" si no se invierte en capacitar al personal de forma adecuada.

10 de junio

El Financiero.

Baja 48% suplantación de identidad en bienes raíces de Nuevo León.

Nuevo León registró una baja de 48 por ciento en los delitos de suplantación de identidad y documentos apócrifos en las operaciones del sector inmobiliario, durante el periodo de 2017 a 2018 y se espera que se mantenga en estos niveles para el lapso de 2018 a 2019, esto a raíz de los protocolos de seguridad que han implementado el Colegio de Notarios Públicos y el Registro Público de la Propiedad en el estado.

Héctor Mauricio Villegas Garza, presidente del Colegio de Notarios Públicos del estado, comentó que a pesar de las 20 leyes que hoy en día tienen que revisar un notario público antes de proceder a notarial una operación de compraventa de un inmueble, gracias a esto se ha podido "blindar" dichas transacciones y proporcionarles a los involucrados mayor seguridad.

Comentó que en los últimos años el trabajo administrativo de los notarios se ha incrementado en un 200 por ciento.

La Asociación Mexicana de Profesionales Inmobiliarios (AMPI) Monterrey organizó un panel sobre los riesgos y delitos inmobiliarios.

"Hoy en día las leyes que regulan una compraventa de inmueble son: Ley de notariado, código civil del estado, código de procedimientos civiles, ley de propiedad en condominio, ley de catastro del estado, entre otras".

Por su parte, Gustavo Cerrillo Ortiz, miembro de la comisión de enlace con la AMPI Monterrey, enumeró los medios por los que se realizan fraudes inmobiliarios: falsificación de documentos; suplantación virtual; blanqueo de documentos apócrifos y transmisión por coacción.

Para Daniel Cebrián, presidente de AMPI Monterrey, es importante que los asesores inmobiliarios estén cada vez más preparados e informados.

Por ello, se ha firmado un convenio de colaboración entre AMPI y el Colegio de Notarios Públicos de Nuevo León para evitar fraudes inmobiliarios.

"Este convenio es el primero que se firma en Monterrey y la idea es que se pueda extender a nivel nacional donde participen todos los estados (...) Este convenio es para apoyarnos mutuamente e ir profesionalizando cada vez más la asesoría inmobiliaria. Nos vamos a ayudar mucho en la capacitación con los Notarios Públicos. Hay asesores que quieren aprender", indicó.

11 de junio

El Financiero.

Advierten de agencias de viajes “fantasmas”.

Con el fin de evitar fraudes de agencias “fantasmas” contra viajeros de Nuevo León y otros estados del país, la Asociación Nacional de Agencias de Viajes (ANAV) puso en marcha la campaña “Agencias de Viajes con Rostro”.

Sandra Lozano de Martínez, presidenta de esta agrupación, y Tulio Bernal Ramírez, director de este proyecto, señalaron que en esta campaña participan 51 agencias de viajes, algunas con una trayectoria de hasta 50 años, pero esperan que se incorporen más empresas serias y formalmente registradas para contrarrestar estos fraudes.

Señalaron que, de acuerdo con la Procuraduría Federal del Consumidor, en 2017 se interpusieron 525 quejas a nivel nacional contra agencia de viajes “fantasmas”, en el 2018 subieron a 860 y en lo que va del 2019 se han interpuesto ya 715 demandas.

“Estas empresas cometen fraudes de miles y miles de pesos, euros y hasta dólares, de manera frecuente y sin sanción alguna”, dijo Guadalupe Mendoza, integrante del consejo directivo de la ANAV.

Los directivos recomendaron a los viajeros que antes de comprar un paquete de viaje se acerquen a una agencia profesional para que no los vayan a engañar.

Señalaron que las agencias de viajes serias y profesionales cuentan con un registro de la Secretaría de Turismo y trabajan con la NOM Oficial Mexicana 10.

La mayoría de las agencias de viajes “fantasmas” operan a través de páginas en Facebook, donde ofrecen viajes con rebajas exorbitantes.

11 de junio

El Universal.

Detienen a individuo por cometer fraude al interior del Metro.

Un sujeto de 22 años fue detenido por cometer fraude al interior del Sistema de Transporte Colectivo (STC) Metro, pues ofrecía locales comerciales en estaciones de la red de forma fraudulenta, identificándose como trabajador del organismo con una credencial apócrifa.

"La Subgerencia de Administración de Permisos Administrativos Temporales Revocables del Sistema de Transporte Colectivo Metro es la única entidad que puede otorgar a una persona física o moral el uso, aprovechamiento y/o explotación de uno o varios espacios locales, por lo que exhorta a los usuarios a evitar caer en fraudes" informó el Metro.

Tras su detención, once personas identificaron al inculpado y aseguraron que el sujeto se comprometió a entregarles espacios comerciales a cambio de dinero, sin que a la fecha cumpliera con la entrega.

Una mujer, argumentó que entrego cien mil pesos al hombre, quien presentaba una credencial institucional del Metro falsa. Otra persona señalo, que entregó al presunto inculpado la cantidad de setenta mil pesos. Nueve personas mas denunciaron el engaño, sin indicar la cantidad de dinero que entregaron.

El defraudador operaba en las estaciones de correspondencia, Pantitlán, Hidalgo y Pino Suárez, donde permanecía junto a los locales desocupados y, con algunos documentos en mano, ofrecía de forma verbal los espacios a cambio de renta que iban de cinco a quince mil pesos mensuales.

"El STC Metro lleva a cabo una supervisión exhaustiva de los PATR, a fin de verificar que todos cumplan con las normas establecidas para su funcionamiento, de lo contrario son suspendidos" explico.

12 de junio
Milenio.

Lanzan protocolo para la protección de cuentas bancarias.

Para evitar el fraude y los robos de cuentas bancarias, la Fiscalía General del Estado y la Secretaría de Seguridad Pública de Coahuila, iniciaron la actualización del protocolo de actuación para la protección de usuarios de instituciones bancarias en la región.

Bajo la coordinación del Mando Especial para La Laguna y con la presencia de distintas firmas de sucursales crediticias, se analizaron los hechos relacionados con la vulnerabilidad que se genera entorno a los cuentahabientes, previo, durante y posterior a la realización de una operación financiera.

Se expusieron los factores de riesgo y las medidas precautorias para evitar ser víctimas de un delito. Gerardo Márquez Guevara, fiscal general de Coahuila, dio a conocer una serie de recomendaciones para que la ciudadanía tome las medidas necesarias. Con el apoyo de Seguridad y Protección Bancaria (Seproban), se estableció la colaboración directa de instituciones bancarias locales y compartir información vital para el seguimiento de un hecho delictivo, así como el acceso a material videográfico, que servirán como mecanismos de datos de prueba en las investigaciones.

Aunque este fenómeno se presenta en gran parte del país, en La Laguna, se busca evitar el crecimiento de esta incidencia.

¿Qué debo hacer para evitar un fraude o robo?

Se recomienda adoptar medidas preventivas, al acudir a un banco o cajeros automáticos como evitar uso de equipos celulares, gorras y lentes oscuros dentro de las sucursales, no compartir información personal con desconocidos de cuentas o tarjetas bancarias, hacer uso de cajeros iluminados y ubicados principalmente en centros comerciales con alta afluencia de personas.

En caso de hacerlo en la noche, acudir en compañía de una persona de confianza y contar con tarjetas de identificación debidamente firmadas. Añadieron que una buena opción es optar por medios electrónicos o banca en línea, a través de aplicaciones móviles y el pago mediante tarjetas. Finalizaron con que, ante cualquier situación de riesgo o caso de sospecha, reportarlo de inmediato al Sistema de Emergencia 911.

14 de junio

El Economista.

Yalitza Aparicio advierte fraude en reventa de boletos para la Guelaguetza.

Los boletos de la Guelaguetza 2019 se han agotado en menos de dos semanas y debido al aumento de la demanda de las entradas a esta tradicional muestra de culturas y bailes del estado de Oaxaca, los costos de alcanzaron una oferta de hasta 30,000 pesos en reventas por internet.

Sitios como Viagogo y Stubhub fueron evidenciados en redes sociales triplicando los precios para este evento para los dos primeros lunes del mes de julio.

Al respecto la Procuraduría Federal del Consumidor (Profeco) en Oaxaca evidenció que las plataformas digitales incurrieron en presuntas prácticas desleales en la reventa de boletos; cuando el gobierno estatal confirmó la conclusión de la comercialización de estos.

Además de que, según el exhorto del gobernador, Alejandro Murat, debido al éxito de este año hará la propuesta a la Cámara de Diputados el siguiente año para que sea abierta una tercera fecha de esta festividad, algo nunca antes visto.

La investigación que reveló Profeco en el estado apuntó que la demanda de compra de las entradas a la máxima fiesta de los oaxaqueños se debió a la presencia, y creencia, de que la actriz Yalitza Aparicio, recientemente nominada a un Premio de la Academia por su interpretación en la película Roma, bailaría con la delegación mixteca, sin embargo, esta información fue desmentida por la propia actriz mediante sus redes sociales.

"Sobre una reventa de boletos para la Guelaguetza a elevados precios para verme bailar. Yo no voy a bailar en la Guelaguetza", aseguró Aparicio.

Mientras que Fernando Rosales García, integrante del comité de autenticidad que acredita la participación de las delegaciones en la Guelaguetza desaprobó que terceros utilicen el nombre de la oaxaqueña como un "gancho" para lucrar.

También recomendó a las personas interesadas en adquirir boletos para la festividad de la Guelaguetza se abstengan de comprarlos en este momento, debido a que pueden ser objeto de fraude, debido a que las localidades están agotadas.

15 de junio

El Economista.

Hackers usan Google Calendar para promover ofertas fraudulentas.

Los ciberdelincuentes siempre buscan formas para estafar a las personas sin que éstas se den cuenta. Por ello, importante compañía de ciberseguridad alertó sobre un nuevo fraude que ataca a los usuarios mediante notificaciones apócrifas en el Calendario de Google para obtener información sobre sus plásticos y cuentas bancarias. En un comunicado, la empresa advirtió que este fraude, denominado phishing de calendario, se detectó durante mayo. Los hackers enviaban invitaciones a eventos no solicitados, aprovechando la utilidad de que la aplicación agrega citas a los calendarios del usuario automáticamente.

El fraude se produce cuando el estafador envía una invitación no solicitada al calendario que contiene un enlace de phishing. Entonces aparece una notificación de la invitación en la pantalla de inicio del teléfono y recomienda al destinatario hacer clic en el enlace. En la mayoría de los casos, se redirigía al usuario a un sitio web con un cuestionario simple que ofrecía premios en efectivo.

Para poder recibir dicha recompensa, se le solicitaba un pago de trámite, para el que tenía que ingresar detalles de su plástico y agregar sus datos personales. Los estafadores utilizaban dichos datos para robo de identidad y vaciar las cuentas del cliente. “La estafa del calendario es una estratagema muy eficaz, pues la gente está más o menos acostumbrada a recibir mensajes de spam en correos electrónicos o a través de mensajes instantáneos y no confían de inmediato en ellos. Pero puede que este no sea el caso cuando se trata de la aplicación de calendario, cuyo propósito es organizar la información del usuario”, aseveró investigadora de ciberseguridad.

De acuerdo con la experta, es posible evitar este engaño, desactivando de manera automática los eventos en el Calendario de Google. Para ello, deberá abrir esta función, y en la parte de configuración dar clic en el ícono del engrane y luego en configuración de eventos. Posteriormente se desplegará un menú de opciones, elija agregar invitaciones automáticamente, y seleccione “No, solo mostrar las invitaciones a las que he respondido”.

Debajo de esto, en la sección ver opciones, asegúrese de que “Mostrar eventos rechazados” no esté marcado, a menos que específicamente desee verlos. “La buena noticia es que no es necesario tomar medidas complejas para evitar este tipo de estafa, pues la función que la hace posible se puede desactivar fácilmente en la configuración del calendario”, aseguró investigador de ciberseguridad.

La especialista dijo que jamás se debe ingresar información personal si no tiene seguridad de que el sitio web que visita cuenta con las medidas de seguridad necesarias.

El spam y el phishing explotan vectores de ataque no tradicionales que pueden ser lucrativos para los ciberdelincuentes, pues tienen la posibilidad de engañar a usuarios experimentados que tal vez no caigan con amenazas comunes.

15 de junio

Excelsior.

¿Qué es el código CVV o CVC de tu tarjeta de crédito?

Actualmente todas las tarjetas de crédito y débito tienen un código CVV o CVC, el cual, se ubica en la parte trasera del plástico. Son tres números que funcionan como método de seguridad para evitar fraudes.

El código funciona para realizar transacciones cuando la tarjeta no está físicamente presente, por ejemplo, cuando son compras por Internet o teléfono.

CVV es Card Verification Value (Código de Valor de Verificación o Validación), y son los números que se ubican en la parte trasera de la tarjeta, en el lugar de la firma.

CVC es Card Verification Code (Código de Verificación de Tarjeta), tiene el mismo uso que el CVV, pero cambia de nombre, dependiendo de las empresas que emiten la tarjeta de crédito.

Adicional, hay otro tipo de CVV, el cual se encuentra en la banda magnética, el cual, se activa al momento de hacer la compra. En otros casos, al momento de leer el chip, el consumidor debe poner su NIP en la terminal punto de venta, para autorizar la compra.

La desventaja de un CVV en la cinta magnética, es que cuando los delincuentes la copia, se llevan con ella el código activo, y esto es lo que les permite hacer cargos al titular de la tarjeta.

Por supuesto, adicional al candado de los códigos CVV o CVC, existe la fecha de vigencia, como medida de seguridad extra, para realizar compras a distancia.