# Boletín de Fraude 15 de septiembre 2020

01 No dejes que te roben tu dinero por i nternet o por teléfono (II).

02 Si adquiere un crédito, verifique que la entidad esté debidamente registrada.

03 Advierten por fraudes en Playa del Carmen.

04 Si realiza algún trámite con su afore, no sea víctima de fraude .

05 Estiman pérdidas de 16 mil mdp por fraude cibernético.

06 Los biométricos y el SAT.

## ¿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

# No dejes que te roben tu dinero por internet o por teléfono (II).

**02 septiembre 2020**

El Economista.

(**Segunda y última parte)**

En la primera parte hablamos del phishing que es la manera más común como los delincuentes buscan robar nuestra información por Internet (o por teléfono), haciéndose pasar por una institución financiera (o de otro tipo) o bien empleados de la misma.

Pero no es la única manera para robarse nuestras claves. Existen otras que también son comunes, como instalar un malware en una computadora (la nuestra o una de uso compartido). Hay varios tipos de malware, entre ellos, programas instalados que espían y registran todo lo que hacemos en esa máquina, incluyendo todo lo que tecleamos.

Hay personas que tienen sus contraseñas en una hoja de cálculo o en el bloc de notas, todo esto es fácil de robar y de hackear. Incluso al navegar en redes públicas, como las de un café, puede haber manera de que alguien se meta por la red a nuestra máquina sin que nos demos cuenta.

¿Cómo proteger entonces nuestra información? A continuación algunas sugerencias:

1. Nunca acceder a portales bancarios ni poner información personal o contraseñas en computadoras compartidas. En nuestro propio equipo, tener software antivirus y antimalware instalado y actualizado.

2. Cuando estemos en redes públicas (ejemplo en un restaurante o aeropuerto) siempre activemos un VPN para navegar (en general pero sobre todo cuando tengamos que acceder a un sitio seguro). Esto nos permite hacerlo de manera privada y garantizar que no hay otros ojos que nos estén espiando en esa red. Existe una enorme variedad de opciones, unas más seguras que otras. Personalmente uso NordVPN.

3. Usar contraseñas seguras y únicas en cada sitio, de más de 10 caracteres, con letras mayúsculas, minúsculas, números y símbolos. Esto significa: no usar la misma contraseña en dos bancos, o en nuestro mail, ni tampoco en la oficina.

Lamentablemente muchos bancos en México, de manera increíble, no tienen una política de contraseñas seguras y no permiten introducir símbolos o bien más de ocho caracteres. Hagamos siempre lo mejor que nosotros podamos.

Si es una contraseña fácil, como nuestro cumpleaños, cualquiera la podría adivinar sin mucho esfuerzo. Si la repetimos y usamos la misma en varios lados, si alguien la obtiene podrá acceder a todos los diferentes sitios y manipular nuestra información.

El correo electrónico muchas veces es un medio para recuperar contraseñas olvidadas: ahí mismo necesitamos una contraseña única y sumamente segura.

¿Cómo recordarlas todas? Podemos usar softwares como 1password o LastPass, entre otros, que generan contraseñas seguras, las mantienen de forma encriptada y nos permiten acceder de manera sencilla a cada sitio web desde una computadora o dispositivo móvil.

---

Paseo de la Reforma 243 Piso 18 Suite 16 Col. Cuauhtémoc 06500 México D.F. Conmutador 6729- 8070 Fax: 5511.2500

protiviti®
Face the Future with Confidence

# No dejes que te roben tu dinero por internet o por teléfono (II). (Continuación)

**02 septiembre 2020**

El Economista.

4. Usar en la medida de lo posible 2FA (autenticación de dos factores) que no es más que una contraseña dinámica. Un token del banco es una forma de 2FA, pero hay otras generadas mediante una app como Authy o Google Authenticator (el mismo password puede también almacenarlas). Servicios como Gmail, twitter y muchos otros, tienen 2FA.

5. Jamás dar clic a ligas o links que recibimos a través de correos electrónicos o mensajes de texto. Siempre ingresar directamente al banco, a través de su página de internet (teclear nosotros la dirección) o bien a través de la aplicación móvil oficial. Es el consejo más simple y el más poderoso para evitar el phishing.

6. Si recibimos un mensaje o llamada diciendo que nuestra tarjeta fue bloqueada, antes de dar cualquier información, es mejor terminar la interacción y llamar directamente al banco (al número que aparece al reverso de nuestra tarjeta). Así nos aseguramos de estar hablando realmente con alguien de la institución.

protiviti®
Face the Future with Confidence

# Si adquiere un crédito, verifique que la entidad esté debidamente registrada.

**03 septiembre 2020**

El Economista

Cuando adquiere un financiamiento o crédito con su banco tiene la confianza de que, al ser una institución reconocida, existe una garantía de que el proceso de contratación y otorgamiento del mismo es seguro, sin embargo aún hay personas que se dedican a realizar fraudes haciéndose pasar por instituciones financieras, y al encontrar a sus víctimas, ofrecen créditos atractivos con pocos requisitos como un "gancho" para llamar la atención, pero detrás de ello hay una estafa.

Actualmente y debido a la crisis provocada por el coronavirus, muchas personas recurren a diversas instituciones para adquirir un financiamiento, por lo que el riesgo de ser engañado aumenta, incluso en días recientes, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) alertó a la población debido a que detectó supuestas empresas que hacen uso fraudulento y suplantación de nombres de Sociedades Financieras de Objeto Múltiple (Sofomes) en diferentes estados de la República Mexicana, incluida la Ciudad de México. "Ante la recurrente práctica de suplantar la identidad de entidades financieras para defraudar a las personas que buscan contratar un crédito rápido, sobre todo en estos momentos de dificultades ante los efectos provocados por la pandemia, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), alerta de nueva cuenta a la población en general de la existencia de empresas ficticias que se ostentan como entidades financieras a través de las redes sociales, páginas de Internet apócrifas o anuncios en periódicos", aseveró en un comunicado.

En el caso de la capital del país, la Condusef detalló que cuatro sofomes y una sofom, que se encuentran registradas y resultaron afectadas, denunciaron ante la comisión el uso indebido de sus nombres. Por lo general, los defraudadores solicitan un anticipo previo a la "entrega" del crédito, muchas de estas empresas fraudulentas son anunciadas a través de llamadas telefónicas, páginas de Internet y en los últimos años, en redes sociales como Facebook o Whatsapp.

De acuerdo con los casos detectados, la Condusef informó que las personas defraudadas han pagado y perdido cantidades que van de los 1,000 a los 100,000 pesos por lo que han acudido al Ministerio Público a presentar la denuncia correspondiente.

**Razón social, la clave para detectarlas**

¿Cuáles son las empresas que han suplantado el nombre de las sofomes y la sofom registradas? La comisión detalló que en el caso de la CDMX, las empresas que fueron detectadas como falsas son: Desarrollo Empresarial Ain; Corporación Financiera de América del Norte COFIDAN; ION Financiera; Konfío Red Amigo e InterOpcion las cuales utilizan la misma razón social (a excepción de Red Amigo, que utiliza un nombre similar) por lo que es importante verificar ante la propia Condusef cuáles son las originales.

El modus operandi que usan se basa en ofertar créditos con pocos requisitos para obtenerlo, sin embargo solicitan un pago como garantía para "apartar" el crédito, la Condusef indicó que generalmente piden 10% del monto total del crédito solicitado y que, al realizar el pago del anticipo en una cuenta bancaria o por depósito en tiendas de conveniencia, las víctimas tratan de contactar a la supuesta entidad sin éxito, es ahí cuando descubren que se trata de un fraude.

protiviti®
Face the Future with Confidence

# Advierten por fraudes en Playa del Carmen.

**07 septiembre 2020**

El Financiero.

Un grupo de inversionistas regiomontanos y de la Ciudad de México (CDMX), advirtieron de una estafa que sufrieron en la compra de departamentos en Playa del Carmen Quintana Roo, por parte de la empresa GMB.

GMB es una empresa que se dedica a la comercialización de diversos proyectos inmobiliarios en todo el estado de Quintana Roo.

Señalaron que por un lado incumplieron en la entrega a tiempo de departamentos desde el año pasado y los clientes "no ven para cuando" avance el proceso, en la negativa de respuesta a la petición de la devolución de su dinero, y en otros casos en la no entrega de los rendimientos acordados en el contrato.

El representante legal de varios de los afectados, refirió que el 28 de febrero de 2019, uno de sus clientes, (que prefirió el anonimato), firmó un contrato de promesa de transmisión de propiedad con la sociedad Desarrollo 1540 SA de CV, a través del cual adquiriría uno de los departamentos del complejo.

"Toda la operación desde el contacto, envío de documentación y pagos se hizo a través del personal de GMB, empresa que comercializó exclusivamente dicho proyecto, refirió la fuente".

Explicó que en el contrato de promesa de transmisión de propiedad se estableció como fecha de entrega el 30 de junio de 2019 con un periodo de gracia de 90 días, que vencieron el 30 de septiembre.

"Visité el edificio en diversos meses de junio a octubre de 2019 y vi la obra completamente detenida. Contacté a personal de GMB para ver qué sucedía y se empezaron a desentender, que ellos sólo comercializan y no tienen responsabilidad por la obra y otras excusas.

"Pedí la recisión del contrato y que me regresaran el dinero entregado. Me pidieron contactar a representante legal de Desarrollo 1540, a quien el 6 de noviembre de 2019 le envié un correo electrónico en el que notificaba el incumplimiento de contrato y le pedía la devolución correspondiente y no he tenido ninguna respuesta", explicó el cliente.

Al día de hoy, la obra sigue detenida y sin avance alguno, aseguró la fuente, por lo que el 8 de julio pasado presentó reclamación en la Profeco, para notificar el incumplimiento de dicho contrato.

En total son 24 departamentos con diferentes clientes y no hay quién les brinde una solución.

Personal de ventas de GMB, confirmó que Desarrollo 1540 está parado, "hasta que no esté el semáforo en verde van a poder reiniciar debido al Covid".

protiviti®
Face the Future with Confidence

# Si realiza algún trámite con su afore, no sea víctima de fraude.

**07 septiembre 2020**

**El Financiero.**

La Consar reitera que todos los trámites del SAR son gratuitos; tiene la oportunidad de interponer una queja directamente con su administradora.

Los fraudes son una forma en la que, a través de diversas estafas, los delincuentes obtienen ventaja sobre sus víctimas al engañarlas.

Sus métodos son diversos, desde los tradicionales de persona a persona, hasta los más recientes, donde con ayuda de la tecnología basta con sólo abrir un mensaje en su correo electrónico donde su información y datos personales corren peligro.

La situación se agrava cuando se involucran temas de información bancaria o con trámites personales, por lo que es importante identificar cuando se trata de una estafa con el fin de no ser una víctima más.

En días recientes, la Condusef lanzó una alerta sobre empresas fraudulentas que suplantan el nombre de diversas entidades financieras, sin embargo, en esta ocasión la Consar también ha advertido a aquellos trabajadores que realizan trámites en su afore, ya que se detectó que existen algunos "agentes promotores" que estafan a personas a la hora que éstas buscan realizar algún movimiento con su administradora.

La premisa que debe conocer es que, todos los servicios que otorga el SAR son gratuitos, por ejemplo, en el caso de un retiro parcial por desempleo o cambio de afore. Hace unos días, el presidente de la Consar se pronunció al respecto en su cuenta de twitter.

La propia comisión ha reiterado que carece de atribuciones para conocer y resolver los presuntos hechos irregulares cometidos por una persona ajena al SAR.

El modus operandi de los estafadores es sencillo, únicamente se acercan a aquellas personas que, en busca de asesoría o ayuda para llevar a cabo un trámite en su administradora, solicitan una cantidad de dinero a cambio de realizar dicho trámite en su cuenta afore.

"Es un tema donde, de entrada, se representan a sí mismos como unos 'solucionadores del asunto', generalmente te abordan afuera de alguna oficina de la afore, se promueven por las redes sociales y anuncian que ellos te gestionan el retiro de tus recursos al 100%, te dicen que no vas a tener ningún problema, muchos ofrecen sus servicios en despachos donde arreglan todos estos asuntos y dicen que van a meter una demanda al Seguro Social y a la afore para que puedas tener tu saldo; finalmente esto no es así. No se necesita un trámite jurídico para recuperar estos recursos que son tuyos", dijo un experto en pensiones.

Detalló que los gestores muchas veces se aprovechan del desconocimiento o preocupación de las personas, por lo que es importante que, si identifica un caso de este tipo recurra directamente a su afore.

"Si alguien le pide datos lo tiene que notificar a su afore, es importante hacerlo. Hoy, como los trámites digitales están basados en información biométrica, difícilmente alguien tomará o tendrá acceso a su información a menos que tú se las brindes, pero sí es importante que la gente tenga conciencia que no debe proporcionar datos personales", aseveró.

.

protiviti®
Face the Future with Confidence

# Estiman pérdidas de 16 mil mdp por fraude cibernético.

Los consultores de Seguridad de la Información (CSI) estimaron pérdidas de hasta 16 mil millones de pesos en fraude cibernético, derivado del aumento de compras y comercio electrónico en el país durante este año.

**08 septiembre 2020**

Milenio.

Durante la conferencia virtual "Retos y riesgos de la ciberseguridad en la nueva normalidad", el director del Área de Consultoría y Servicios de Seguridad de CSI, destacó que hasta 2019 el fraude cibernético había dejado pérdidas de 11 mil 171 millones de pesos, ahora ante la pandemia de covid-19 y con la nueva normalidad podrían ascender a 16 mil 756 millones de pesos, lo que significa un aumento de 49.9 por ciento.

El especialista en cibernética sostuvo que los ciberataques en el campo de ingeniería social han aumentado "considerablemente", entre los que se encuentran llamadas telefónicas falsas en líneas de banca con 45 por ciento de aumento, correos electrónicos falsos con 35 por ciento, así como el comercio falso con un incremento de 30 por ciento.

"Realmente son una preocupación, es el ataque de ingeniería social, en donde predominan las llamadas telefónicas falsas de bancos, principalmente con distintos bancos, es decir, utilizan la suplantación de identidad para hacer el ataque", dijo. Indicó que después de la crisis sanitaria por covid 19 aumentó en 80 por ciento el uso de internet y 50 por ciento del uso de la banca para compras, por lo que podría causar mayores reclamaciones por fraude cibernético.

De acuerdo con la Comisión Nacional para la Protección de Usuarios de Servicios Financieros (Condusef), para 2018 el fraude cibernético dejó pérdidas por 9 mil 517 millones de pesos, para 2019 fueron 11 mil 171 millones de pesos, lo que representa un incremento de 17.3 por ciento.

El director del Área de Consultoría y Servicios de Seguridad de CSI llamó al gobierno federal a priorizar aprobación de la Ley General de Ciberseguridad, presentada como iniciativa en el Senado, con la finalidad de atacar los ciberataques en el país y sancionar a quien los cometa.

"Este tipo de acciones ayudan, estamos en un proceso inicial de tema de ley y falta mucho para que pueda tener una diferencia en la proporcionalidad de los ciberataques, pero a futuro esperemos que se agilice y de 3 a 6 meses pueda disminuir el tema de ciberataques en el país", afirmó.

protiviti®
Face the Future with Confidence

# Los biométricos y el SAT.

**10 septiembre 2020**

**El Financiero.**

La base de datos biométricos gremial que la banca trabaja desde hace tiempo parece que ya no sólo va tomando forma, sino que incluso todo indica que será posible que tengan acceso en el próximo año a una de las bases gubernamentales que estaban interesados en checar que es la del Servicio de Administración Tributaria (SAT).

Actualmente los bancos trabajan y pagan por verificar en tiempo real con el Instituto Nacional Electoral (INE) las huellas dactilares que tienen de más de 90 millones de mexicanos en su base de datos y con la cual checan si el nuevo cliente o actual, coinciden sus huellas con las que tienen en el INE. Así ha salido corriendo más de un 'cliente' evitando robo de identidad, por ejemplo, o vaya a saber que otro fraude.

Bueno, ahora el SAT pide permiso para ofertar el 'servicio de verificación de identidad de los usuarios' tanto a entes privados como públicos, ya que asegura que cuenta con más de 100 millones de huellas dactilares, más de 20 millones de iris y más de 15 millones de rostros, todos bajo los estándares biométricos establecidos por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) que es técnicamente también parte de las certificaciones que deben cumplir los bancos.

El servicio —asegura— sería dado para que se pueda hacer una comparación automatizada con huellas recabadas por otros entes públicos o privados “que cuenten con la infraestructura tecnológica necesaria para el procesamiento y petición automatizada de confirmación de identidad conforme a la información biométrica que transmitan” y la respuesta al igual que con el INE sería al verificarse las huellas, si está o no, en su base de datos.

La validación será a partir de los elementos que sean enviados y emitirá sólo la respuesta de la coincidencia o no de la información biométrica, por lo que dice no se comparten datos personales, pero el detalle que se ve y que ya es analizado por especialistas en el tema, es que los datos biométricos fueron entregados con un fin en particular a una institución pública, que ahora al igual que el INE todo indica que podría cobrar por ese servicio de verificación de identidad.

Lo cierto, es que hay otras bases de datos biométricos en poder y uso del gobierno federal como el IMSS; la Secretaría de Relaciones Exteriores también con la emisión de pasaportes y de seguir el mismo camino. La integración de estas bases podría ser un paso positivo para tratar de frenar el robo de identidad e incluso ayudar a crear una identificación oficial más completa y segura; lo malo es que una vez más los millones de mexicanos que entregamos esos datos a entidades públicas podrían lucrar con ellas. En fin, nada es perfecto y todo tiene un costo.

# Los biométricos y el SAT. (Continuación)

**10 septiembre 2020**

**El Economista.**

Y ya que hablamos del SAT, para quienes no siguen los reportes financieros ni los temas legales y fiscales, quizás esté causando sorpresa el que empresas e instituciones financieras parece que están en un desfile de pagos de adeudos al fisco “doblando las manos”, pero la realidad es que son muchos y por miles de millones los temas de interpretaciones fiscales que se litigan cada día. Ayer, por ejemplo, un banco  informó que acordó pagos complementarios porque justamente había diferencias de criterio en temas relacionados con el ISR de siete ejercicios fiscales y pagó alrededor de 450 millones por cada uno de ellos, pero en esos años pagó más de 43 mil millones de pesos sólo de ese impuesto donde los datos son públicos.

En 2018 y 2019 pagó sólo de ISR 40 mil millones de pesos.

En general, dentro del sistema financiero, los bancos son los que mayor aporte de impuestos hacen. Ahí están los reportes financieros públicos, lo malo que este año, por la caída de la economía y el hecho de que difirieron créditos y en el caso del banco hasta los intereses, el aporte que harán al fisco será mucho, mucho menor. Por lo pronto, la moneda está en el aire.