Protege tu identidad

Cuidar tu información personal y financiera es la mejor arma contra el robo de identidad. No te conviertas en una víctima más.

ROCÍO **ALVEAR**

En las películas y en las caricaturas es común ver que los superhéroes hacen hasta lo imposible por mantener protegida su identidad y a pesar de que son personajes de ficción no están tan apartados de la realidad, pues el aumento desmedido de fraudes ligados al robo de identidad, hace esencial que estemos alerta para evitar convertirnos en una víctima más de este delito.

Sin darte cuenta, todos los días realizas actividades financieras: consultar el saldo de tu plástico en algún cajero automático o por internet, comprar boletos para el cine o un concierto por teléfono, pagar la cuenta en un restaurante con tarjeta, entre muchas otras que al realizarlas revelan parte de tu información como los números de tus tarjetas de débito o crédito, tu nombre, domicilio, teléfono, etcétera, y aunque no lo parezca cada uno de estos datos son una mina de oro para un ladrón de identidad, pues los aprovechan para cometer algún fraude en tu nombre sin que lo notes.

¿Qué es el robo de identidad?

Cuando alguien roba tu información personal y financiera, con la finalidad de suplantar tu identidad para obtener beneficios de forma fraudulenta, se dice que comete *robo de identidad*.

Tus datos pueden ser utilizados para solicitar créditos o usar los que ya tienes de forma exagerada, crear cheques falsos con tu número de cuenta e incluso obtener a tu nombre algún documento oficial. Cuando esto sucede, no sólo pierdes dinero, también se daña tu reputación financiera. Si solicitan un crédito a tu nombre sin que te des cuenta y por consiguiente nunca se paga, esto dañará tu historial crediticio y es probable que en el futuro las instituciones financieras te nieguen algún crédito. En casos más graves puedes tener problemas con las autoridades, derivados de algún fraude o infracción que el ladrón cometa a tu nombre.

Por lo general, a las víctimas les lleva mucho tiempo darse cuenta de que su identidad ha sido robada y cuando se percatan del fraude, el ladrón ya ha hecho estragos.

Tus datos están protegidos

¿Sabías qué el IFAI está facultado para sancionar a quienes hagan mal uso de tus datos? Todas las entidades que manejan datos personales deben otorgar medidas de seguridad y establecer mecanismos para que los usuarios accedan, rectifiquen, cancelen o puedan oponerse al manejo de su información personal. La Ley Federal de Protección de Datos Personales regula la forma y las condiciones en que las empresas (bancos, hospitales, universidades, etc.) deben utilizar los datos personales de sus clientes. Para mayor información consulta **www.ifai.org.mx**

Lamentablemente existe una gran variedad de métodos que emplean los ladrones para acceder a tu información, desde los más simples como el robo de tu cartera hasta los más sofisticados, que utilizan tecnología de punta para traspasar las medidas de seguridad de tus cuentas bancarias. Para que no seas víctima de este fraude, te explicamos las modalidades de robo que existen y te damos algunos consejos para manejar con cautela tus datos.

Robo de carteras y bolsos

Éste es quizá el truco más viejo de todos. Muchas personas llevan consigo no sólo sus identificaciones oficiales como la licencia de conducir, también tarjetas de crédito y/o débito, comprobantes de operación como consultas de saldo en cajeros automáticos, comprobantes de domicilio, toda esta información facilita que roben tu identidad.

Carga solamente lo indispensable, revisa tu bolso y cartera todos los días y saca aquello que no te haga falta. Evita traer contigo más de una tarjeta. Si sabes que ese día no realizarás ningún pago con el plástico, mejor guárdala en casa, en un lugar seguro.

Cuida tu buzón

Basta con extraer del buzón de tu casa recibos para el pago de servicios (luz, teléfono, agua, telefonía celular), solicitudes de tarjetas de crédito pre-aprobadas y estados de cuenta bancarios para que alguien utilice tu documentación con el propósito de solicitar algún crédito a tu nombre o

Toma nota

Menos papel, más seguro

Paperless es un servicio que se ha vuelto cada vez más popular en instituciones financieras, consiste en sustituir el envío en papel de tus estados de cuenta —a tu domicilio— por el envío de éstos a tu correo electrónico. Así evitas que alguien robe tu correspondencia y se apropie de tu información bancaria, además contribuyes con el cuidado de la naturaleza.

hacer uso de tus cuentas bancarias para cometer un fraude.

Para prevenir esta situación revisa tu correo diariamente, mantente al pendiente de las fechas en que recibes tus estados de cuenta y si no te llegan comunícate a tu banco. Si vas a salir de vacaciones pídele a alguna persona de confianza que recoja tu correo.

Búsqueda en basureros

Se conoce en inglés como *dumpsterdiving* y se trata de buscar en la basura restos de estados de cuenta bancarios, recibos o *vouchers* de tarjetas de crédito, talones de cheques, propagandas y promociones ligadas a tarjetas bancarias.

Antes de tirar a la basura algún documento que tenga información personal o financiera, destrúyela por completo y verifica que ningún dato pueda ser extraído. Tampoco se trata de guardar por siglos estados de cuenta de tarjetas que incluso ya cancelaste; si es mucho el papeleo que conservas en casa, cómprate un pequeño triturador de papel, para poder deshacerte de él.

Cuando acudas a un cajero automático llévate siempre los comprobantes de operación, nunca los dejes en los botes de basura que se encuentren por ahí.

Un extraño te vigila

El espionaje por encima del hombro se da cuando un delincuente te espía sin que lo notes mientras usas el cajero automático o tecleas en una computadora los datos de tu cuenta, NIP o contraseña. También pueden escucharte cuando indicas tu número de tarjeta de crédito o datos de identificación por teléfono al realizar alguna consulta de saldo a tu banco.

Cuando utilices tus plásticos en público o llenes algún tipo de formulario con tu información personal debes tener cuidado con las personas que se encuentran a tu alrededor. Con los avances que hay en la tecnología –celulares y cámaras- pueden tomar una fotografía de tu tarjeta, o incluso un video cuando tecleas tu NIP en el cajero.

Pharming

Es similar a la pesca de datos, te llega un correo electrónico que al momento de abrirlo instala un código en tu equipo personal, modificando determinados archivos, para que la próxima vez que ingreses al portal de tu banco te desvíen a sitios web falsos sin que te des cuenta, aunque escribas correctamente la página. Por eso, es más difícil detectar el *pharming* que el *phishing*, ya que el primero no necesita que la víctima acepte un mensaje señuelo. La entrada del código malicioso en tu sistema también puede realizarse por medio de descargas que hagas por internet o a través de unida-

No dejes tu información en mano de terceros

Si acudes a alguna institución a solicitar un crédito, te piden documentación personal y al final no te lo otorgan o decides desistir, no dejes tus papeles en manos de extraños.

¡Recógelos!

des de almacenamiento removibles como una memoria USB.

¿Cómo prevenir este fraude? Instala en tu computadora paquetes de seguridad que te protejan contra virus y otras amenazas, actualízalos con regularidad. Estos paquetes deben incluir un *firewall*, programa que verifica que no tengas *spyware* (software espía) o *adware* (programas que muestran publicidad web), ambos pueden causar el reenvío a la página fraudulenta.

Además siempre que hagas uso de la banca por internet o entres a algún comercio virtual donde te soliciten los datos de tus tarjetas para realizar un pago, verifica que la dirección que aparece en la barra del explorador comience con https (la "s" significa que la página es segura) y que en la parte inferior o superior del navegador aparezca un candado. Nunca ingreses a un sitio web por medio de hipervínculos.

Toma nota

Utiliza el sentido común

Si una persona, un sitio web o un correo electrónico te prometen una oferta especial o te informan que ganaste un premio, utiliza el sentido común: por lo general si algo suena demasiado bueno para ser verdad, probablemente no lo es.

No proporciones información personal por correo electrónico ni por internet, a menos de que tengas la certeza de que el sitio al que estás ingresando es legítimo. Busca sus políticas de privacidad, éstas describen el uso que la página le dará a la información personal que proporciones en ella (si será provista a terceros). Si no encuentras la política de privacidad o no la entiendes considera abandonar este sitio.

Si utilizas equipos públicos (*cibercafés*) o accedes a internet por medio de redes inalámbricas desprotegidas (*WiFi*), evita realizar operaciones a través de la banca en línea; hazlo mejor desde tu hogar.

Pesca telefónica

Algunas veces el defraudador utiliza un marcador automático para llamar a cierta cantidad de números telefónicos, cuando la llamada se contesta una grabación se activa y alerta al "consumidor" que su tarjeta de crédito está siendo utilizada de forma fraudulenta y que debe llamar a determinado número telefónico de inmediato. Cuando la víctima habla a ese número, responde otra grabación que le indica que su cuenta necesita ser verificada y le solicita que ingrese mediante el teclado telefónico los 16 dígitos de su tarjeta de crédito. A este fraude se le denomina *vishing*.

Otro tipo de estafa se da a través del celular; utilizan los mensajes de texto (SMS) para enviar vínculos de sitios web falsos en los cuales te solicitan verificar los datos de tu cuenta, a este fraude se les conoce como *smishing*.

Si recibes una llamada donde te solicitan teclear tus datos o te piden información ¡cuelga! Los bancos no piden ese tipo de información por teléfono, por mensajes de texto o por correo electrónico. Llama a tu banco marcando el número de teléfono que viene en tu tarjeta de crédito o en tu estado de cuenta. Cuando recibas un mensaje de texto extraño bórralo y nunca des clic en los vínculos que te envíen por este medio.

Éstas son sólo algunas de las formas en que opera el robo de identidad, pues día a día los delincuentes inventan nuevos métodos. Por eso es importante estar alerta y seguir las medidas de seguridad recomendadas.

¿Y si ya caíste?

Si detectas que tu identidad ha sido robada o que se ha hecho mal uso de tus datos financieros, denuncia el fraude ante el Ministerio Público. Si tu tarjeta de crédito fue clonada, cancélala de inmediato y acude al banco a resolver el problema.

Si no obtienes respuesta por parte de tu banco dentro de los siguientes 45 días naturales, acude a la Condusef. Llama al 5340 0999 en el D.F o al 01800 999 8080 para el resto de la República mexicana.

Si robaron tu identidad para la contratación de un servicio a tu nombre, por ejemplo de telefonía celular, debes acudir a Profeco, comunícate al teléfono 5568 8722 en el D.F. o al 01800 468 8722 del interior.

Si derivado de este fraude, se reporta una mala nota en tu historial crediticio, presenta una solicitud de aclaración ante las Sociedades de Información Crediticia (Círculo de Crédito y Buró de Crédito). Si por alguna razón no procede, puedes solicitar que en tu reporte de crédito se incluya, de forma gratuita, un texto de hasta 200 palabras explicando tu inconformidad.

Preocúpate si:

- No recibes los estados de cuenta de tus tarjetas de crédito o de cheques.
- Al momento de solicitar un crédito no te lo otorgan por un mal historial crediticio (y nunca has incumplido con tus pagos).
- En tu reporte de crédito aparecen préstamos que no solicitaste a compañías con las que no tienes ningún tipo de relación.
- Te llegan facturas por cuentas que no tienes o cargos en tu tarjeta por algún artículo que no compraste.
- Recibes llamadas de cobradores o de compañías de servicios que no contrataste.

¡Puedes ser víctima de fraude!