Consejos de protección durante las vacaciones

El robo de entidades es a menudo un delito de oportunidad. No sea un turista que le presenta esa oportunidad a un delincuente. Su información personal, tarjetas de crédito y débito, licencia de conducir, pasaporte y otra información personal son el objetivo del estafador. Dedicar unos minutos a planificar antes de viajar puede ayudar a reducir el riesgo de que un estafador arruine sus vacaciones.

Llame a su banco y a las compañías de tarjetas de crédito para informarles cuándo y dónde viajará.

Para proteger su identidad mientras está de vacaciones, aquí le ofrecemos algunos consejos:

- Limpia su billetera. Elimine las tarjetas de crédito innecesarias, además de no llevar su tarjeta de Seguro Social y otros documentos innecesarios que podrían comprometer su identidad en caso de pérdida o robo durante sus vacaciones.
- Lo mejor es llevar dos tarjetas de crédito. Llevar demasiadas tarjetas de crédito lo someterá a una preocupación adicional si pierde o le roban su billetera. Pero existe un riesgo al llevar una sola tarjeta de crédito si, por ejemplo, su tarjeta se desactiva inadvertidamente debido a una sospecha de fraude o si la banda magnética se daña. Si esto sucediera estando fuera de casa, podría convertirse en un gran dolor de cabeza.
- Fotocopie o haga una lista del contenido restante de su billetera. Guárdelo en un lugar seguro y cerrado con llave o con una persona de confianza en su casa a quien pueda contactar en caso de que pierda o le roben su billetera.
- No deje su billetera, ni ningún documento que contenga información personal, al descubierto, en su habitación de hotel. Las habitaciones de hotel no son los lugares más seguros. Muchas personas tienen acceso a la habitación. Utilice la caja fuerte del hotel cuando esté disponible.

- Llame a su banco y a las compañías de tarjetas de crédito para informarles cuándo y dónde viajará. Sus departamentos de fraude pueden monitorear sus cuentas en busca de transacciones no autorizadas durante este tiempo. También se recomienda que conozca su número de identificación personal (PIN) antes de viajar; si su PIN es de seis dígitos, solicite a su institución financiera que lo convierta a un PIN de cuatro dígitos que será más aceptado mientras viaja al extranjero.
- Muchos países, incluidos los de Europa, utilizan tarjetas con chip y PIN o EMV; estas tarjetas utilizan un microchip y un número de identificación personal (PIN) integrado en el chip para validar las transacciones. Una tarjeta de crédito emitida en EE. UU. sin chip ni PIN aún se puede usar mientras se viaja, pero generalmente solo en ubicaciones con un asistente de ventas. Muchas ubicaciones, como máquinas expendedoras de billetes, carreteras de peaje y surtidores de combustible, requieren tarjetas con chip y PIN.
- Deje su chequera en un lugar seguro bajo llave en su casa.
- Utilice tarjetas de crédito en lugar de tarjetas de débito. Esto reduce su vulnerabilidad a que se

vacíe su cuenta corriente mientras está de vacaciones. Las tarjetas de débito y las tarjetas de crédito tienen diferentes plazos y responsabilidades para el consumidor en materia de informes de fraude; consulte con su banco para obtener más detalles.

- Guarde los recibos de sus tarjetas de crédito y los contratos de alquiler de automóviles, especialmente si contienen el número completo de su tarjeta de crédito.
- Si planea usar una tarjeta de cajero automático durante sus vacaciones, use una que no tenga privilegios de tarjeta de débito (por ejemplo, una que requiera un PIN y no contenga el logotipo de Visa o MasterCard). Puede pedirle a su banco que cambie una tarjeta de cajero automático/débito por una que sea "solo cajero automático". Lo mejor es utilizar cajeros automáticos que se encuentran en bancos o cooperativas de crédito y que se encuentran en zonas bien iluminadas. Asegúrese de examinar cuidadosamente el cajero automático para detectar signos de manipulación. Esté atento a cualquier cosa que parezca sospechosa; un simple tirón del lector de tarjetas o un movimiento del teclado ayudará a identificar posibles dispositivos de robo o cajeros automáticos alterados. También busque cámaras pequeñas o poco visibles, que puedan ser colocadas sobre el teclado con el propósito de obtener su PIN. Recuerde siempre cubrir las manos cuando ingrese su PIN, es la forma más fácil de protegerse de una cámara oculta o de alguien que mire por encima del hombro.
- Cuando coma en un restaurante, esté atento a su tarjeta de crédito cuando pague la factura. Si el dependiente quita su tarjeta de la vista, existe la posibilidad de que puedan crear un "clon" utilizando un copiador de tarjeta portátil que copiará la información de la banda magnética de la tarjeta.
- Muchos restaurantes han instalado terminales de pago de mesa o tabletas de autoservicio para permitir a los consumidores pagar su factura directamente en la mesa. Esto podría mejorar la seguridad de la tarjeta de crédito al garantizar que su tarjeta nunca salga de su posesión, limitando el riesgo de que su tarjeta sea “clonada” o incluso que la deje accidentalmente en el establecimiento. Asegúrese de leer atentamente las instrucciones, pregunte sobre las “tarifas” por el uso del servicio y asegúrese de que su transacción esté completamente procesada antes de partir.
- Pídale a su oficina de correos o a un vecino de confianza que guarde su correo. El correo que se deja en un buzón desbloqueado es una mina de oro para los ladrones de identidad. Un buzón lleno también envía una señal a posibles ladrones de que su casa está vacía.
- Si trae consigo su computadora portátil, tenga mucho cuidado al usarla para acceder a la banca en Internet u otros servicios protegidos con contraseña, a los que pueda acceder desde redes Wi-Fi. Asegúrese de utilizar “puntos de acceso” Wi-Fi que sean seguros.
- Tenga en cuenta que los registradores de teclas (software que puede rastrear sus pulsaciones de teclas) pueden rastrearlo cuando utiliza cibercafés, centros de negocios de hoteles u otras instalaciones de acceso público a Internet en lugar de llevar su propia computadora portátil. Las instalaciones de acceso público podrán utilizar servidores que no estén cifrados. Por lo tanto, nunca acceda a información confidencial desde una computadora pública.
- Sea siempre cauteloso con la información que comparte en los sitios de redes sociales. De la misma forma que usted no pondría un cartel en la puerta de tu casa que dijera "Me he ido de vacaciones". Cuando usted anuncia sus planes de viaje en las redes sociales, hace exactamente eso, pero, electrónicamente. Esta información puede ser utilizada por delincuentes que sabrán que usted estará fuera de casa.
- Active la autenticación de dos factores si se ofrece. La autenticación de dos factores es una capa adicional de seguridad que combina algo que tienes, un token físico como una tarjeta o un código, con algo que sabes, algo memorizado como un número de identificación personal (PIN) o una contraseña.

(Información extraída de la hoja informativa *Planning a Summer Vacation?* de *Privacy Rights Clearinghouse*

Para obtener más información o poner una queja, visite nuestro sitio web o contáctenos:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Correo electrónico: DATCPHotline@wi.gov
Sitio Web: datcp.wi.gov
Teléfono: (800) 422-7128 TTY: (608) 224-5058

IDTheftVacationSPANISH992 (rev 1/24)