Tarjetas de crédito

Si hace compras en línea o por teléfono, puede pagar con su tarjeta de crédito. Ya que no puede usar la tarjeta misma, probablemente proporcionará el número de su tarjeta de crédito, incluyendo la fecha de caducidad, por teléfono o Internet. Si estos números llegan a manos equivocadas podría descubrir cargos no autorizados en el siguiente estado de cuentas de su tarjeta de crédito.

- Haga negocios sólo con compañías que conoce; no dé el número de cuenta de su tarjeta de crédito para hacer una compra o una reservación, a menos que usted haya iniciado la transacción.
- Compre sólo de sitios web seguros que usen software de encriptación para transferir datos de su computadora al comerciante y que tengan políticas estrictas de privacidad y seguridad.
- No responda a mensajes electrónicos que parecieran provenir de la compañía que emitió su tarjeta de crédito pidiéndole una "actualización" de su información. Llame directamente a la compañía para verificar la información que se necesite.
- Si recibe ofrecimientos de tarjetas de crédito preaprobadas por correo, no los tire en la basura sin antes hacerlos pasar por una máquina desfibradora.
- Si está esperando recibir por correo nuevas tarjetas de crédito y éstas demoran en llegar, o si no recibe sus cuentas de cobro en el período de tiempo esperado, llame inmediatamente a la entidad emisora de la tarjeta de crédito.
- Después de realizar compras por Internet, revise cuidadosamente los estados de cuenta de sus tarjetas de crédito durante varios meses. Si descubre compras que no hizo, póngase en contacto inmediatamente con la compañía que emitió la tarjeta de crédito y formule un reclamo por los cargos.
- Obtenga una copia de su reporte de crédito una vez al año y revíselo buscando cualquier actividad no esperada.

Notificación de un problema

Si descubre que hay cargos no autorizados en el estado de cuentas de su tarjeta de crédito o retiros de su cuenta bancaria, notifique inmediatamente a la policía y a la institución financiera correspondiente. Si es víctima del delito de robo de identidad, formule una denuncia policial; presente una denuncia en línea a la Comisión de Comercio Federal (Federal Trade Comission) en **www.consumer.gov/idtheft/**; notifique a las tres agencias de crédito más importantes: Equifax (**www.equifax.com**), Experian (**www.experian.com**) y Trans Union (**www.transunion.com**) y cierre su cuenta.

Consejos para prevenir delitos del

NATIONAL CRIME PREVENTION COUNCIL
1000 Connecticut Avenue, NW
Thirteenth Floor
Washington, DC 20036-5325
202-466-6272
www.ncpc.org

y de

Bureau of Justice Assistance

La Campaña Nacional de los Ciudadanos para la Prevención del Crimen (The National Citizens' Crime Prevention Campaign) patrocinada por la Coalición Estadounidense para la prevención del Crimen (Crime Prevention Coalition of America) y financiada principalmente por la Dirección de Asistencia Judicial (Bureau of Justice Assistance), Oficina de Programas de Justicia (Office of Justice Programs), Departamento de Justicia de los EE.UU.

La producción de este folleto fue posible gracias a una subvención de ADT Security Services, Inc., Tyco International Ltd. Company.

2005

Protección de su información privada

NATIONAL CRIME PREVENTION COUNCIL

El correo electrónico, Internet, los cajeros automáticos (automated teller machines – ATM), la banca en línea, los teléfonos celulares, las compañías telefónicas de larga distancia e incluso las tarjetas de crédito hacen nuestra vida más eficiente. Sin embargo, a medida que nos integramos más con la tecnología, se hace más difícil mantener nuestra información privada confidencial. Las transacciones electrónicas pueden dejarlo vulnerable al robo de identidad y a otros tipos de fraude. Los siguientes consejos sencillos le pueden ayudar a mantener segura su información privada.

Contraseñas

Frecuentemente se requieren contraseñas para tener acceso a información de instituciones financieras, médicas y de otro tipo. Los piratas informáticos ("hackers") tienen herramientas sofisticadas para descifrar códigos. Los siguientes son consejos para crear y proteger sus contraseñas.

- Seleccione por lo menos ocho símbolos, incluyendo una combinación de letras, números y signos que usted pueda recordar pero que otros no puedan adivinar fácilmente.
- No use el nombre de soltera de su madre, el nombre de su cónyuge, los últimos cuatro dígitos de su número de Seguro Social, nombres de sus hijos o mascotas, ni la fecha de su nacimiento.
- No use ninguna palabra que pueda hallarse en el diccionario de cualquier idioma.
- Cree una nueva contraseña para cada sitio web o para ingresar a un sistema de computadoras que lo solicite. Si eso es poco práctico, cree unas cuantas contraseñas difíciles de adivinar y úselas en los sitios en los que desee mantener más seguridad. Cree contraseñas fáciles de recordar para usarlas en sitios menos importantes.
- Cambie sus contraseñas con regularidad, por lo menos una vez al mes.
- Memorice sus contraseñas; si tiene que escribirlas, no las lleve escritas en su billetera ni las deje en lugares sin protección, incluyendo archivos de la computadora.
- Si su computadora le brinda la opción de recordar su contraseña, no elija esa opción.
- No comparta sus contraseñas con miembros de su familia, amigos o colegas.
- Si ha ingresado su clave de acceso a un cajero automático o está comenzando la sesión en una computadora, asegúrese de que nadie esté mirando mientras ingresa su contraseña.

Números de identificación personal

El número de identificación personal (personal identification number – PIN) es uno de los métodos usados por los bancos y las compañías telefónicas para proteger su cuenta del acceso no autorizado. Un PIN es un código privado emitido al titular de la tarjeta para permitirle el acceso a esa cuenta. Usted puede proteger su número PIN siguiendo estos consejos:

- Memorice su número PIN y no se lo dé a nadie, incluyendo a miembros de la familia o empleados del banco.
- Nunca escriba su PIN en las tarjetas de los cajeros automáticos (ATM) o tarjetas para hacer llamadas de larga distancia; no lleve su número PIN en su cartera o billetera.
- Cuando use un cajero automático (ATM) o un teléfono público, sitúese frente al teclado del cajero automático o del teléfono público para evitar que nadie observe su PIN mientras lo ingresa.
- No deje su recibo en la máquina cuando use el cajero automático; los delincuentes pueden usarlo para obtener su número de cuenta.
- Si un banco u otra institución le asigna un número PIN que consta de los cuatro dígitos finales de su número de Seguro Social, pida que se los cambien por otros números.

Números del Seguro Social

Algunas empresas y agencias del gobierno afirman que usar su número de Seguro Social (Social Security number – SSN) es la manera más precisa de almacenar y recuperar información. Su número de Seguro Social es, sin embargo, el objetivo principal de delincuentes interesados en cometer robo de identidad y otros delitos más. Por lo tanto, es esencial que proteja su SSN.

- Dé su SSN sólo cuando sea absolutamente necesario. Los empleadores necesitan su SSN para informar al Servicio Interno Fiscal (Internal Revenue Servicie – IRS) sus ingresos, pero las agencias del orden público no lo necesitan para emitirle un permiso de estacionamiento.
- No lleve su tarjeta de Seguro Social en su billetera o cartera a menos que lo necesite para una situación específica, como por ejemplo el primer día en un trabajo nuevo.
- No imprima su SSN en cheques o tarjetas profesionales de presentación.
- De ser posible, no incluya su SSN en los formularios de aplicación para puestos de trabajo.
- Si le piden su SSN en línea, busque el símbolo de candado cerrado en la parte inferior de la página y lea las normas de privacidad de la compañía con respecto a la forma en que protege su información personal.
- No responda a mensajes electrónicos no solicitados que pidan su SSN y otra información personal. Ninguna compañía acreditada ni agencia gubernamental envía mensajes electrónicos no solicitados para pedir datos personales confidenciales.
- Si una empresa privada le pide su SSN, sugiera alternativas como su número de licencia de conducir (a menos que su número de licencia de conducir sea el mismo que su SSN).
- Si la Dirección General de Tránsito de su estado usa el SSN como el número de licencia de conducir, pida un número diferente.