office of neighborhood involvement

Fomentamos una cultura de participación cívica conectando y apoyando a todos los residentes de Portland que colaboran entre sí y con el gobierno para crear vecindarios y comunidades inclusivos, seguros y habitables.

1221 SW 4th Avenue, Suite 110
Portland, Oregon 97204

tel 503-823-4000
fax 503-823-3050
teletipo 503-823-6969

Amanda Fritz
Comisionada de la Ciudad

Amalia Alarcón de Morris
Directora

Línea de información y derivaciones
de la Ciudad y del Condado

503-823-4000
•
Este documento está disponible en el sitio Web de ONI:

www.portlandonline.com/oni/cp

Robo de identidad

Cuando alguien enloda su buen nombre

Programa de Prevención de Delitos de la Oficina de Participación Vecinal
Primavera de 2010

El robo de identidad se produce cuando una persona utiliza la información personal de otra, tal como su nombre, número del Seguro Social o su información financiera personal para cometer fraude u otros delitos. Para las víctimas del robo de identidad, restaurar su buen nombre y su clasificación crediticia puede ser una tarea muy difícil y que exigirá de mucho tiempo. La prevención es mucho más sencilla.

Cómo se produce el robo de identidad

MANERAS EN QUE LOS LADRONES OBTIENEN SU INFORMACIÓN PERSONAL

- Obtienen la información de negocios o de otras instituciones apoderándose de los registros o de la información mientras trabajan allí, sobornando a los empleados para que les den acceso a dichos registros, accediendo a los registros electrónicos mediante la piratería, u obteniendo la información de los empleados mediante artimañas.
- Podrían robar la correspondencia tales como estados de cuenta bancarios, ofertas de tarjetas de crédito y cheques nuevos en blanco.
- Podrían robar la cartera (billetera) o sustraer la información personal de la vivienda.

Tarjetas clonadas, estafas por Internet o por teléfono y buscadores de basura.

Los ladrones de identidad podrían robar los números de las tarjetas de crédito o de débito apoderándose de la información en un dispositivo de almacenamiento de datos conectado a un cajero automático (ATM) como parte de una práctica conocida como "*skimming*" (clonación). Podrían sustraer información personal a través de correos electrónicos estafadores ("*phishing*") o por teléfono ("*pretexting*") haciéndose pasar por empresas legítimas que dicen que la persona tiene problemas con su cuenta. Los ladrones de identidad rebuscan la basura, a lo cual se le conoce como "*dumpster diving*".

Cómo prevenir el robo de identidad

SEGURIDAD DE LAS CUENTAS

- Aplique contraseñas a sus tarjetas de crédito, a sus cuentas bancarias y telefónicas. Evite utilizar información que pueda obtenerse fácilmente como su apellido materno, su fecha de nacimiento, los cuatro últimos números de su tarjeta de Seguro Social o su número de teléfono, o una serie de números consecutivos.
- Guarde en un lugar seguro la información personal que tenga en su vivienda, sobre todo si alguien más vive con usted, utiliza servicios externos o cuando alguien vaya a hacer trabajos a su vivienda.
- Pregunte acerca de los procedimientos de seguridad con respecto a la información en su centro laboral, en negocios, en consultorios médicos o en otras instituciones que tengan información que lo identifique a usted. Averigüe cómo la información se dará a saber a otras personas o entidades.
- No dé su información personal por teléfono, a través del correo o por Internet, a menos que usted haya iniciado el contacto o esté seguro de saber

quién es la persona con la que está tratando. Antes de dar su información personal, cerciórese de estar tratando con una organización legítima.
- Deposite la correspondencia que va a enviar en los buzones de recolección de la oficina de correos o en la oficina de correos de su localidad, y no en un buzón de correos que no sea seguro.
- Rompa o triture recibos de tarjetas de crédito, copias de solicitudes de crédito, formularios de seguro, informes médicos, cheques y estados de cuenta bancaria, tarjetas de cargo vencidas que esté desechando y ofertas de tarjetas de crédito que reciba por correo. Si desea optar por no recibir ofertas de tarjetas de crédito por correo, llame al 1-888-5-OPTOUT.
- No lleve consigo su tarjeta del Seguro Social; déjela en un lugar seguro.
- Proporcione su número del Seguro Social (SSN, por sus siglas en inglés) sólo cuando sea absolutamente necesario. Si alguien le pide su SSN, pregunte para qué lo necesita y cómo será utilizado. Pregunte de qué manera se le protegerá de robos y qué sucederá si usted no proporciona su SSN.
- Cuando pida cheques nuevos, vaya a recogerlos al banco en vez de que se los envíen por correo.

SEGURIDAD DE LA COMPUTADORA
- El software de protección contra virus debe actualizarse con regularidad y los parches para el sistema operativo de su computadora u otros programas de software deben instalarse para que esté protegido de intrusiones e infecciones que pudiesen exponer los archivos y las contraseñas en su computadora.
- No abra los archivos que haya recibido de desconocidos, ni haga clic sobre los hiperenlaces, ni descargue programas de personas que no conoce.
- Emplee contraseñas “sólidas” que combinen letras (mayúsculas y minúsculas) con números.
- Utilice un programa contrafuegos (*firewall*) si usa una conexión a Internet de alta velocidad que deja su computadora conectada a Internet las 24 horas del día, para impedir el acceso de personas ajenas a su computadora.
- No realice transacciones financieras de ninguna clase en Internet, a menos que emplee un navegador seguro que cifre o que codifique la información delicada. Opte por “https” en vez de “http” en la barra de la dirección, y fíjese si hay un icono en forma de candado cerca de la parte inferior de la ventana del navegador.
- Consulte las políticas de seguridad de los sitios Web si tiene preguntas sobre cómo se mantiene la precisión, el acceso, la seguridad y el control de la información personal que colecta el sitio, la manera en que se empleará y si se proporcionará a terceros.

Si es usted víctima del robo de identidad

ACCIÓN INMEDIATA
- Presente una alerta de fraude ante las agencias de reporte crediticio y revise sus reportes crediticios. Las alertas de fraude ayudan a evitar que el ladrón que robó su identidad abra más cuentas en nombre de usted. Comuníquese con una de las tres agencias crediticias:
  Equifax: 1-800-525-6285; www.equifax.com
  Experian: 1-888-397-3742; www.experian.com
  TransUnion: 1-800-680-7289; www.transunion.com
- Cierre las cuentas que sepa o que crea han sido manipuladas indebidamente o que hayan sido abiertas de forma fraudulenta.
- Haga la denuncia en la comisaría cerca de donde vive o cerca del lugar en que ocurrió el robo de identidad.
- Presente una queja ante la Comisión Federal del Comercio (*Federal Trade Commission*). Visite *www.ftc.gov/idtheft* o llame al 1-877-438-4338 para presentar su queja.
- Obtenga una copia de la publicación “Tome control: Defiéndase Contra el Robo de Identidad” de la Comisión Federal de Comercio (vea la información de contacto provista) y siga las sugerencias sobre cómo recuperarse del robo de identidad.

MÁS INFORMACIÓN SOBRE EL ROBO DE IDENTIDAD

Para obtener información con más lujos de detalle sobre la prevención del robo de identidad y cómo resolverlo, visite *www.ftc.gov/idtheft* Esta hoja informativa es simplemente un resumen de los consejos prácticos que se proporcionan en ese sitio con respecto al robo de identidad.