

Las Maneras Efectivas Para Prevenir El Robo de Identidad



División de Protección a la Comunidad Oficina del Fiscal del Condado de Boulder

Prevenga el Robo de Identidad por Teléfono, en el Hogar o por Correo

Por teléfono:

- **No conteste llamadas** de números desconocidos, anónimos o bloqueados, o cuando no reconoce el número que aparece en su identificador de llamadas.
- **Comparta lo menos posible de su información:**
 - **NUNCA comparta información personal** como su número de Seguro Social o información bancaria o de tarjeta de crédito con alguien que le llame inesperadamente, sin importar quien dicen ser.
 - Solo ofrezca información personal por teléfono cuando **usted haga la llamada** y esta seguro a quien le está llamando.
- Pida a sus proveedores de línea telefónica información sobre como bloquear llamadas: muchos proveedores ofrecen estas características gratuitamente.
- Asegúrese de estar en la lista nacional y de Colorado de “no llamar” (no-call) para su hogar y su celular.

En el hogar y por correo:

- **Revise sus estados de cuenta y facturas cuidadosamente:**
 - Reporte discrepancias a su institución financiera inmediatamente.
- **Guarde y descarte documentos sensibles sabiamente:**
 - Procure tirar la basura el día que lo recogen, no antes.
 - Triture documentos que contengan información sensitiva personal o información financiera.
 - Considere pagar sus facturas y revisar sus estados de cuenta de forma electrónica.
- **Proteja su correo:**
 - Recoja su correo del buzón tan pronto pueda.
 - Envíe correo importante desde la oficina postal o envíelo certificado--no ponga correo saliente en su buzón.
- **Presente sus impuestos temprano** para impedir que ladrones de identidad de impuestos puedan presentar con su información con la esperanza de conseguir un su reembolso.
- **Tome medidas para monitorear y salvaguardar su crédito:**
 - Solicite y revise su reporte de crédito: Es gratis semanalmente en www.AnnualCreditReport.com.
- **Considere pedir una alerta de fraude o un congelamiento de reporte de crédito:**
 - Una alerta de fraude requiere que un negocio verifique su identidad antes de emitir un crédito nuevo, mientras que un congelamiento de crédito restringe el acceso a su reporte de crédito.

Para preguntas, llame a la División de Protección a la Comunidad (303) 441-3700

Prevenga el Robo de Identidad en Línea

Manejo de contraseña:

- Utilice contraseñas **largas, únicas y fuertes**: cámbielos **frecuentemente**.
 - Las contraseñas para el trabajo, los medios sociales y cuentas financieras **NO DEBEN SER IGUALES**.
 - **Nunca reúse** contraseñas viejas.
 - Cambie las contraseñas de sus computadoras **en casa, los módems y los enrutadores** periódicamente también.
- **Considere usar una “frase”:**
 - Use una frase que le sea familiar, pero cambie algunas letras por mayúsculas, números y símbolos.
 - Una frase puede ser más fácil de recordar y más difícil que otra persona lo adivine.



Tener conciencia de sus correos electrónicos:

- **No conteste** a los correos cuando no reconoce al remitente.
 - **Nunca haga clic en los enlaces o los archivos adjuntos** en cualquier correo electrónico que no haya solicitado, sin importar quien diga que lo manda.
 - **No muerda el anzuelo** y haga clic en las cajas que dicen “click here” en los correos electrónicos pretendiendo ser de alguna agencia que necesita su información o que su información ha sido comprometida (compañía de tarjeta de crédito, banco, Amazon, eBay etc.).
 - En vez de contestar a un correo electrónico de este tipo, **usando el número en su estado de cuenta o tarjeta de crédito**, entre a su cuenta de la compañía en línea y **use su nombre de usuario y contraseña**.
- **Tenga cuidado con los correos electrónicos que dicen venir de algún “amigo” quien necesita un favor**, o que indica que el amigo o algún pariente esta en problemas y necesita ayuda.
 - Elimine correos electrónicos provenientes de algún “amigo” quien pide dinero, números de tarjetas de identificación, cuentas bancarias, o tarjetas de crédito o débito. **Llame al amigo** para dar seguimiento.



Consejos para todos sus aparatos u en línea:

- Programe las actualizaciones para que **se instalen automáticamente** en su celular o su computadora cuando estén disponibles.
- Considere usar autenticación multifactorial para sus aparatos, el internet, y sitios de web, especialmente en donde guarda información de salud o financiera.
- Revise su perfil y las configuraciones de privacidad en medios sociales periódicamente.
- **Recuerde... el WiFi público no es público!**
 - Cuando este usando el WiFi público, solo vaya a sitios que no pidan contraseña o información personal o financiera.



Michael Dougherty, District Attorney

BOULDER OFFICE: JUSTICE CENTER · 1777 6TH STREET · BOULDER, COLORADO 80302 · 303.441.3700

LONGMONT OFFICE: 1035 KIMBARK · LONGMONT, COLORADO 80501 · 303.441.3700

WWW.BOULDERCOUNTY.ORG/DISTRICT-ATTORNEY · TDD/V: 303.441.4774

