

Living Safely

with disabilities and special health needs

Cómo protegerme contra el robo de identidad



Children's
Specialized Hospital®

An RWJBarnabas Health facility



Es importante que proteja mi información personal para evitar el robo de identidad. Estas son algunas cosas que puedo hacer para protegerme.

Debo guardar todos mis documentos financieros, las tarjetas del Seguro Social y de Medicare, y otros documentos que tengan mi información personal en un lugar seguro.



Cuando reciba estados de cuenta o documentos en el correo que tengan mi información personal, debo quitarlos de mi buzón lo más pronto que pueda. Esto evitará que otras personas los saquen del buzón.



Si necesito deshacerme de documentos que tengan mi información personal, es importante que los triture antes de desecharlos.

Si no tengo una máquina trituradora de papel, puede haber una compañía en mi ciudad que esté certificada para triturar documentos con información privada.

Si no puedo triturar los documentos, puedo usar un marcador negro permanente para pasarlo sobre mi nombre, mis números de cuentas y cualquier otra información privada. Es una buena idea cortar o romper los documentos después de tapar esta información.



Algunas organizaciones necesitan mi número del Seguro Social para identificarme.

Estas organizaciones incluyen al Servicio de Impuestos Internos (Internal Revenue Service, IRS), mi banco y mi empleador. Estas organizaciones nunca me llamarán y nunca me enviarán correos electrónicos ni mensajes de texto para pedirme mi número del Seguro Social o cualquier otra información personal.



Hay otras organizaciones y compañías que me pedirán mi número del Seguro Social y realmente podrían no necesitarlo. Entre ellas se incluyen proveedores médicos o la escuela de mis hijos.

Debo hacer las siguientes preguntas antes de dar mi número del Seguro Social:

- ¿Por qué necesitan mi número del Seguro Social?
- ¿Cómo protegerán mi número del Seguro Social y cualquier otra información personal?
- ¿Hay una forma de usar números o letras distintos en lugar de mi número del Seguro Social?
- ¿Puede usar solamente los últimos cuatro dígitos de mi número del Seguro Social en lugar del número completo?



Cuando inicie sesión en una cuenta por Internet, debo usar siempre una contraseña que sea difícil de adivinar por otras personas.

Las contraseñas más seguras tienen 12 caracteres, con una mezcla de letras, números y caracteres especiales. Puede ser más fácil recordar una contraseña larga usando un grupo de palabras poco comunes y al azar que sean significativas para mí.



Cuando inicie sesión en una aplicación de mi teléfono o computadora, puede haber un paso más para mantener segura mi información. Esto se llama “autenticación de múltiples factores”.

Dependiendo del sistema, este proceso de autenticación requiere que yo ponga un código o una huella digital, o haga un reconocimiento del rostro o mi contacto visual además de mi contraseña. Este proceso hace más difícil que los estafadores entren a mi cuenta.

The image shows a 'Login' form with a red circle highlighting the password input fields. The form includes a 'Change password' link, a tip about using strong passwords, and three password input fields: 'Current', 'New', and 'Retype new'. The 'New' field has a 'Password strength: Strong' indicator, and the 'Retype new' field has a 'Passwords match' indicator. A 'Save changes' button is located at the bottom.

Login

[Change password](#)
It's a good idea to use a strong password that you don't use elsewhere

Current

New
Password strength: **Strong**

Retype new
Passwords match

[Forgotten your password?](#)

[Save changes](#)

Cuando me pidan que elija preguntas de seguridad, selecciono las preguntas con respuestas que solamente yo sepa.

Trato de evitar las preguntas que pidan información como mi código postal, el apellido de soltera de mi madre y un lugar de nacimiento.

Además, trato de no usar preguntas que tengan una cantidad limitada de respuestas, para que un estafador no pueda adivinar la respuesta.



Nunca le debo dar información personal a ninguna persona que me llame o me envíe correos electrónicos o mensajes de texto.

La persona podría ser un estafador tratando de robar mi información personal.

Si me piden información personal, y no estoy seguro de qué hacer, le hago preguntas y le digo a la persona que llama que volveré a hablarle en otro momento. Esto me dará tiempo para hablar del tema con alguien de mi confianza.

Para más recursos de Living Safely (Vivir Seguro), visite <https://www.rwjbh.org/cshlivingsafely>

Valoramos la experiencia en seguridad de nuestros asociados que hayan demostrado su compromiso con tener comunidades sanas e inclusivas. Algunas partes de este material han sido adaptadas de la Federal Trade Commission (Comisión Federal de Comercio) (www.ftc.gov).

La información incluida en *Vivir seguro con discapacidades y necesidades especiales de salud (Vivir seguro)* se presenta únicamente con fines educativos e informativos. En el contenido se incluye información general: esta podría no reflejar las necesidades individuales o los acontecimientos jurídicos o información actuales de una persona. Children's Specialized Hospital no garantiza, ni expresa ni implícitamente, la precisión, aplicación, adecuación o exhaustividad de la información incluida en *Vivir seguro*, ni en ningún otro sitio web al que esté vinculado. Children's Specialized Hospital específicamente renuncia a toda responsabilidad en relación con las acciones de cualquier persona, realizadas o no, con base en la totalidad o parte de la información u otro contenido de *Vivir seguro*.



Esta iniciativa fue financiada en parte por una subvención del programa Inclusive Healthy Communities Grant Program (Programa de Subvenciones para Comunidades Sanas e Inclusivas) de la División de Servicios para Discapacitados del Departamento de Servicios Humanos de Nueva Jersey.



© 2021 Children's Specialized Hospital