Resumen de la presentación en línea

Australian Government

Be Connected
Every Australian online.

Protección de sus datos personales en Internet (Protecting your personal information online)

Casi todas las aplicaciones, plataformas de redes sociales o sitios web le piden al menos algún tipo de información personal. Su información personal incluye cualquier información o dato que pueda utilizarse para identificarle, como detalles que permitan saber dónde se encuentra o dónde vive, y otros detalles específicos únicos.
Es importante pensárselo siempre dos veces antes de compartir información personal.

La protección de sus datos personales es importante

Proteger su información personal es muy importante, ya que los estafadores y los ladrones de identidad pueden utilizarla para hacerse pasar por usted. Pueden crear cuentas falsas en su nombre y actuar de formas que podrían afectarle ahora o en el futuro. Esto podría incluir fraude, como robar dinero de su cuenta bancaria o pedir un préstamo a su nombre.

Los estafadores pueden utilizar su información por sí sola o en contexto con otra información.
Puede incluir cosas cotidianas que son específicamente suyas, como su:

Información personal

- Nombre y apellidos
- Domicilio
- Número de teléfono
- Fecha de nacimiento
- Número de licencia de conducir
- Datos de su cuenta de banco
- Dirección de correo electrónico
- Nombres de usuario y contraseñas

Documentos de identidad

- Licencia de conducir
- Pasaporte
- Partida de nacimiento
- Tarjeta de Medicare
- Visado australiano o certificado de ciudadanía
- ImmiCard

Sea consciente de lo que comparte

Redes sociales

Es una buena idea evitar compartir información personal en sus cuentas de redes sociales. Los estafadores pueden descubrir mucha información acerca de usted a partir de los datos que comparte en Internet. A veces crean cuestionarios o mensajes con preguntas diseñadas para engañarle y hacerle compartir información personal. Utilizan esta información para adivinar las contraseñas de sus cuentas o para realizar otras estafas especialmente dirigidas a usted.

Utilizar aplicaciones

Sólo descargue aplicaciones de las tiendas de aplicaciones oficiales y lea las políticas de privacidad y reseñas antes de descargar cualquier cosa. También puede limitar la información a la que tienen acceso las aplicaciones. Algunas aplicaciones piden acceso innecesario a sus listas de contactos, cámara, almacenamiento, ubicación y micrófono. Revise y ajuste los permisos de su aplicación en el menú de configuración de su dispositivo inteligente.

Recuerde: Sólo acepte solicitudes de amistad de personas que conozca en la vida real; configure sus cuentas de redes sociales como privadas y revise quién puede ver lo que comparte.

Proteja su información

Utilice la seguridad de los dispositivos

Utilizar software de seguridad en su computadora es una de las formas más sencillas de protegerse y proteger su privacidad. Tener una buena seguridad para su computadora incluye la instalación de programas antiespía (anti-spyware), antivirus y cortafuegos (firewall) de confianza. También debe mantener actualizadas sus herramientas y aplicaciones de seguridad en línea activando las actualizaciones automáticas. Configure el protector de pantalla para que se bloquee automáticamente después de determinado tiempo o para que esté protegido por contraseña. También configure sus dispositivos para que se bloqueen automáticamente si ocurren varios intentos fallidos de inicio de sesión.

Consejo: Una aplicación de gestión de contraseñas también puede ayudarle a crear y almacenar frases de contraseña complejas que sean difíciles de adivinar o hackear. Puede encontrar información sobre **aplicaciones de gestión de contraseñas** y cómo configurarlas en la página web de Be Connected.

Frases de contraseña

Mantenga sus cuentas seguras con frases de contraseñas seguras. Las frases de contraseña son la versión más segura de las contraseñas y se componen de cuatro o más palabras aleatorias.

Intente pensar en una frase de contraseña diferente para cada una de sus cuentas y no recicle partes de ninguna antigua.

Cuando elija su frase de contraseña, esta debe tener las siguientes características:

- **Larga:** al menos 14 caracteres
- **Impredecible:** utilice cuatro o más palabras al azar con números, símbolos y letras mayúsculas y minúsculas
- **Único:** no reutilice sus frases de contraseña

Por ejemplo: Amarillo Asi Hey Planta > Amarill-ASiheyPl@nta!*

Consejo: Compruebe la seguridad de una contraseña utilizando el comprobador de contraseñas del Gobierno de Nueva Gales del Sur en **nsw.gov.au/id-support-nsw/be-prepared/passwords.**

Autenticación multifactor

Siempre es una buena idea activar la autenticación multifactor para sus cuentas. La autenticación multifactor (también conocida como autenticación de 2 pasos) añade una capa adicional de seguridad. Eso significa que, cuando inicia sesión en una cuenta con su contraseña, es posible que se le pida que complete un paso adicional para confirmar que se trate de usted, como introducir un código de un mensaje de texto o utilizar la identificación por reconocimiento facial.

Compre en línea de forma segura

Al comprar por Internet, asegúrese de recurrir a vendedores de confianza y lea las reseñas de otros clientes. Antes de introducir sus datos personales, compruebe que el sitio web utiliza “https” al principio de su nombre de dominio o tiene un icono de seguridad — normalmente un pequeño candado cerrado — en su navegador para indicar que se trata de un sitio web más seguro. Cuando realice una compra, utilice un método de pago seguro como PayPal, BPAY o su tarjeta de crédito.

Utilice una conexión segura

Cuando necesite acceder a cuentas importantes, enviar información confidencial o introducir contraseñas, conéctese a una conexión a Internet de confianza, por ejemplo en casa o en el trabajo, o utilizando los datos de su propio teléfono celular si están disponibles. Las redes Wi-Fi públicas no son tan seguras como las de casa o el trabajo.

Estafas y filtraciones de datos

Protéjase de las estafas

Ser consciente de las estafas y de cómo funcionan es uno de los pasos importantes para evitarlas. Los estafadores fingen pertenecer a una organización o a una persona conocida para intentar engañarle y hacerle proporcionar su información personal. Son las llamadas estafas de suplantación de identidad.

Es importante recordar lo siguiente:

Deténgase: no dé dinero ni información personal a nadie si tiene alguna duda
Los estafadores suelen pedirle que verifique su identidad o que haga un pago.

Piense: pregúntese si el mensaje o la llamada podrían ser falsos
Cuidado con las llamadas, mensajes y correos electrónicos inesperados. Si tiene dudas sobre un mensaje, llame directamente a la organización a través del número de teléfono que figura en su sitio web.

Protéjase: actúe con rapidez si algo va mal
Póngase en contacto con su banco si observa alguna actividad inusual o si un estafador consigue su dinero o información.

Consejo: Visite el sitio web Be Connected para consultar nuestra guía gratuita sobre **estafas de suplantación de identidad** elaborada con Scamwatch.

Filtraciones de datos

Una filtración de datos ocurre cuando alguna información personal que está en poder de una organización se accede o divulga sin autorización, o se pierde. Muchas organizaciones y organismos públicos tienen la responsabilidad legal de informarle si su información personal se ve implicada en una filtración de datos que pueda causarle un perjuicio grave.

Si su información se ve implicada en una filtración de datos, asegúrese de actuar con rapidez y pida asesoramiento a la **Oficina del Comisionado de Información de Australia**. Las medidas que tome dependerán de la información de que se trate. Lleva un registro de lo que hace. También puede obtener apoyo y asesoramiento gratuitos de **IDCARE**.

Para averiguar si un sitio o una aplicación que utiliza ha sufrido una filtración de datos, puede consultar servicios como **haveibeenpwned.com**. Si esto ocurre, cambie inmediatamente sus contraseñas.

Fraude de identidad

Si sabe o sospecha que le han robado su identidad:

- Informe al Centro Australiano de Ciberseguridad de la Dirección Australiana de Señales en **ReportCyber**.
- Póngase en contacto con la policía al 131 444. Pida un informe policial o un número de referencia como prueba de que ha presentado una denuncia.
- Si conoce o sospecha el tipo de información personal que ha sido robada, póngase en contacto con la agencia u organización pertinente para hacérselo saber.
- Comuníqueselo a su entidad financiera lo antes posible.
- Denúncielo al Centro Nacional Antiestafas de **Scamwatch** si forma parte de una estafa.

Tómese su tiempo para explorar Be Connected

Be Connected es un sitio web integral con recursos gratuitos diseñados específicamente para ayudar a los australianos mayores a conectarse a Internet de forma segura y a navegar por el mundo digital con confianza. El sitio también es útil para familias y organizaciones comunitarias que quieran ayudar a miembros mayores de la comunidad a acceder a todas las ventajas de Internet.

Visite beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Este programa ha sido desarrollado por eSafety como parte de la iniciativa Be Connected.