



Australian Government



Actúe ya mismo.
Manténgase a salvo.

Cómo mantenerse seguro en internet

Versión de lectura fácil



Cómo usar esta guía



Somos el gobierno de Australia.

Redactamos esta guía.



Escribimos algunas palabras en **negrita**.

Explicamos el significado de estas palabras.

También hay una lista de estas palabras en la página 28.



Usted puede pedirle a alguien en quien confíe que le apoye para:

- leer esta guía
- encontrar más información.



Esta guía es un resumen de lectura fácil de otra guía.

Incluye solamente las ideas más importantes.



Puede encontrar la otra guía en nuestro sitio web:

www.actnowstaysecure.gov.au

¿Qué contiene esta guía?

Sobre esta guía	4
Mantener seguras sus cuentas	6
Revisar sus ajustes para proteger su información	10
Proteger sus dispositivos	16
Las estafas	20
Alza la voz	25
Lista de palabras	28
Cómo contactarnos	30

Sobre esta guía



Todos debemos pensar en cómo mantenernos seguros en internet.

Se llama **ciberseguridad**.



«Ciber» significa que algo se relaciona con internet.



Esta guía explica algunas cosas que puede hacer para protegerse en internet.

Por ejemplo, de la **ciberdelincuencia**.



La ciberdelincuencia ocurre cuando los delincuentes utilizan internet para cometer delitos.

Por ejemplo, puede que usen internet para:

- robar su información personal
- apoderarse de sus cuentas o perfiles en internet.



La ciberdelincuencia puede ocurrir en cualquier dispositivo, por ejemplo:

- su ordenador,
- su teléfono inteligente
- su reloj inteligente.



Hay ciertas cosas que puede hacer para protegerse de la ciberdelincuencia.



A continuación explicamos qué puede hacer.

Mantener seguras sus cuentas



Debería considerar cómo puede mantener seguras sus cuentas en internet.

Utilizar frases de contraseña robustas y diferentes



Una **frase de contraseña** es un tipo de contraseña más robusta.

Es muy difícil que otra persona la adivine.



Utilizar frases de contraseña robustas y diferentes es una de las mejores formas de proteger sus cuentas.



Debe utilizar una frase de contraseña diferente para cada una de sus cuentas en internet.



Las frases de contraseña incluyen:

- 4 o más palabras aleatorias
- 15 o más letras y números.



Puede incluir algunas mayúsculas.



También puede incorporar algunos símbolos, tales como:

- un guion,
- un signo de dólar
- una arroba.



No debe incluir en sus frases de contraseña ninguna información personal.



Por ejemplo:

- su fecha de nacimiento
- los nombres de sus familiares o mascotas.

Imponer pasos adicionales para acceder a sus cuentas



Puede proteger sus cuentas en internet usando la **autenticación de múltiples factores**, también conocida como **MFA** por sus siglas en inglés.

La MFA implica el uso de 2 o más diferentes maneras de entrar en su cuenta cada vez.



Por ejemplo, tal vez tenga que empezar con su frase de contraseña.

Luego introduce un código que reciba en su teléfono.

Posiblemente pueda elegir entre:



- descargar una aplicación en su teléfono que le dará el código,



- recibir el código en un correo electrónico



- recibir el código en un mensaje de texto.



Con la MFA será más difícil que otros accedan a sus cuentas en internet.

Aunque descubran su frase de contraseña.

Revisar sus ajustes para proteger su información



Puede revisar si sus ajustes están protegiendo su información en internet.



Se incluyen los ajustes de:

- sus cuentas en internet,
- sus dispositivos
- sus aplicaciones.



Usted puede:

- cambiar los ajustes
- elegir cuáles aplicaciones pueden utilizar su información.

Puede encontrar los ajustes de su dispositivo:



- buscando el icono de engranaje
- o
- escribiendo «ajustes» (o «settings» para un dispositivo en inglés) en la barra de búsqueda.



En una aplicación o una cuenta en internet, los ajustes pueden estar dentro del menú.

El menú muchas veces se representa con 3 barras rectas.



Algunos de estos ajustes pueden compartir información sobre:

- quién es usted,
- dónde está
- dónde vive.



Al compartir esta información en internet,
usted puede correr riesgo de ciberdelincuencia.



Los ciberdelincuentes pueden usar su
información para hacerse pasar por usted.

Por ejemplo, pueden usar información tal como:



- dónde vive,



- los nombres de sus familiares



- los nombres de sus mascotas.



Puede configurar sus cuentas para que sus perfiles en las redes sociales sean visibles únicamente para las personas que conoce.

Por ejemplo, su perfil en Facebook.



Estos ajustes normalmente se llaman ajustes de privacidad.



Usted también puede controlar sus **ajustes de localización**.

Los ajustes de localización indican dónde está su dispositivo.



Puede activar o desactivar sus ajustes de localización.

También puede seleccionar cuáles aplicaciones pueden usar sus ajustes de localización.



Puede hacer estas selecciones para:

- sus cuentas en internet,
- sus dispositivos
- sus aplicaciones.

Puede que algunas aplicaciones también le pidan permiso para:



- usar su cámara



- ver sus fotos.



Debe autorizar el acceso a su cámara y sus fotos únicamente para aquellas aplicaciones con las que está familiarizado.

Proteger sus dispositivos



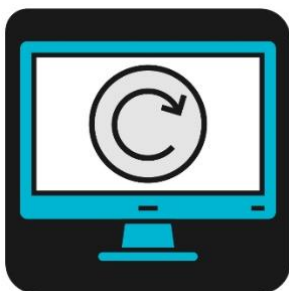
Debe considerar cómo proteger sus dispositivos para mantenerse seguro en internet.

Por ejemplo, su teléfono o reloj inteligente.



Es importante hacerlo para los dispositivos que se conectan a internet.

Actualizar sus dispositivos



Puede actualizar sus dispositivos para mantenerlos seguros en internet.

Por ejemplo, su teléfono y ordenador portátil.



Su dispositivo puede denominarlo una actualización de software.



Las actualizaciones ayudan a los dispositivos a protegerse de la ciberdelincuencia.



Puede configurar un dispositivo para que se actualice automáticamente.



Para aprender más sobre cómo actualizar a sus dispositivos, visite nuestro sitio web:

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Las redes públicas de wifi



Tenga cuidado cuando usa el **wifi público**.



El wifi público es el internet inalámbrico gratuito que se puede usar en lugares públicos.



Por ejemplo, en:

- un café,
- un aeropuerto
- un hotel.



Tenga cuidado con la información que introduzca en un sitio web al usar el wifi público.



Por ejemplo:

- sus datos bancarios,
- sus cuentas de correo electrónico
- sus perfiles en las redes sociales.



Algunos ciberdelincuentes usan el wifi público para:

- ver lo que hace en internet
- robar su información.

Es porque:



- cualquiera puede usarlo



- es más difícil proteger sus dispositivos.



Para aprender más sobre cómo mantenerse seguro cuando usa el wifi público, visite nuestro sitio web:

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Las estafas



Se llama una **estafa** cuando alguien intenta:

- engañarle
- tomar su dinero.



Un **estafador** es alguien que estafa.

Los estafadores pueden tratar de engañarle en:



- un mensaje de texto o llamada telefónica,
- un correo electrónico,
- las redes sociales
- un sitio web.



Pueden parecer simpáticos.

Pero pueden engañarle para que les dé su información.

Pueden utilizar esta información para:



- acceder a sus cuentas en internet,



- hacerse pasar por usted



- robar su dinero.

Los estafadores también pueden:



- crear cuentas falsas para engañarle



- compartir enlaces y anuncios para que haga clic en ellos.

Cómo detectar una estafa

Algo puede ser una estafa si:



- le pide que haga algo rápidamente,



- le ofrece mucho dinero,



- le pide dinero



- le pide que haga clic en un enlace.



Los estafadores también pueden hacerse pasar por una organización que conoce y en que confía.

Por ejemplo, su banco.



Los estafadores lo hacen para que comparta con ellos su información personal.



Deje de hablar con la persona si cree que es estafador.



Debe verificar si la persona es quien dice ser.

Puede contactar con la persona u organización usando los detalles en que confía y que ha encontrado de manera independiente.



Actúe rápidamente para protegerse si algo le parece mal.

Denunciar una estafa



Scamwatch (el organismo de vigilancia contra estafas) ayuda a los australianos a:

- entender las estafas
- denunciar las estafas.



Scamwatch también ayuda a los australianos que se han encontrado con estafas.



Puede denunciar una estafa en el sitio web de Scamwatch:

www.scamwatch.gov.au/report-a-scam

Alza la voz



Debe alzar la voz y hablar de cómo los demás pueden protegerse en internet.

Algunas formas de hacerlo son:



- denunciar la ciberdelincuencia



- compartir sus conocimientos con familiares y amigos.



Explicaremos en las siguientes páginas cómo puede alzar la voz.

Denunciar la ciberdelincuencia

Denunciar la ciberdelincuencia ayuda al gobierno a:



- aprender cómo los ciberdelincuentes tratan de atacar a las personas



- proteger a más personas.



Puede denunciar la ciberdelincuencia en el sitio web ReportCyber:

www.cyber.gov.au/report

Hablar con la familia y amigos sobre la seguridad en internet



Debería compartir con la familia y amigos sus consejos sobre la seguridad en internet.

Usted también puede aprender de ellos.



Puede protegerse a sí mismo y a los demás compartiendo sus conocimientos de la seguridad en internet.



Es importante también si comparte dispositivos con otros.

Lista de palabras

Esta lista explica el significado de las palabras en **negrita** que se encuentran en esta guía.



Ciber

Ciber significa que algo se relaciona con internet.

Ciberdelincuencia



La ciberdelincuencia ocurre cuando los delincuentes utilizan internet para cometer delitos.

Por ejemplo, pueden usar internet para:

- robar su información personal
- apoderarse de sus cuentas en internet.



Ajustes de localización

Los ajustes de localización indican dónde está su dispositivo.



Autenticación de múltiples factores (MFA)

La MFA implica el uso de 2 o más diferentes maneras de entrar en su cuenta cada vez.



Frase de contraseña

Una frase de contraseña es un tipo de contraseña más robusta.

Es muy difícil que otra persona la adivine.



El wifi público

El wifi público es el internet inalámbrico gratuito que se puede usar en lugares públicos.



Estafas

Se llama una estafa cuando alguien intenta:

- engañarle
- tomar su dinero.



Estafadores

Un estafador es alguien que estafa.

Cómo contactarnos



Puede llamar a la línea australiana para la ciberseguridad marcando al:

1300 292 371



Puede visitar nuestro sitio web:

www.actnowstaysecure.gov.au



Puede denunciar la ciberdelincuencia en el sitio web ReportCyber:

www.cyber.gov.au/report



El Information Access Group (Grupo de Acceso a la Información) creó este documento de lectura fácil con fotografías de archivo e imágenes originales. Queda prohibida la reutilización de las imágenes sin autorización. En caso de consultas relacionadas con las imágenes, por favor visite www.informationaccessgroup.com y cite el número de trabajo 6342.
