Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

LA SEGURIDAD EN INTERNET

UNA GUÍA PARA LA TERCERA EDAD

cyber.gov.au

Introducción

Conectarse en línea nos permite mantener el contacto con amigos y parientes, aprender sobre muchos temas e incluso jugar juegos.

Así como nos abrochamos el cinturón de seguridad antes de salir con el coche, debemos tomar medidas para aumentar la seguridad antes de usar internet.

El Centro Australiano de Ciberseguridad (Australian Cyber Security Centre, ACSC) procura comprobar que todos estemos seguros cuando estamos en línea. Este documento presenta algunas prácticas básicas de ciberseguridad que podemos usar para protegernos al navegar por internet.

El Centro Australiano de Ciberseguridad (ACSC) forma parte de la Dirección Australiana de Señales (Australian Signals Directorate, ASD), y proporciona asesoramiento, asistencia y respuestas operativas para prevenir, detectar y responder a los peligros cibernéticos para Australia.
El ASCS vela por que Australia sea el lugar más seguro donde conectarse en línea.
Para obtener más información, guías y asesoramiento sobre la ciberseguridad, visite cyber.gov.au

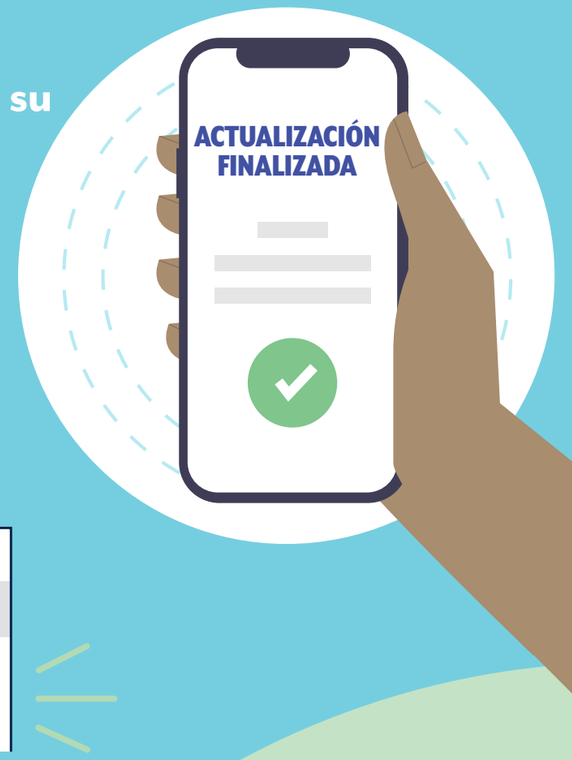
La ciberseguridad para la tercera edad

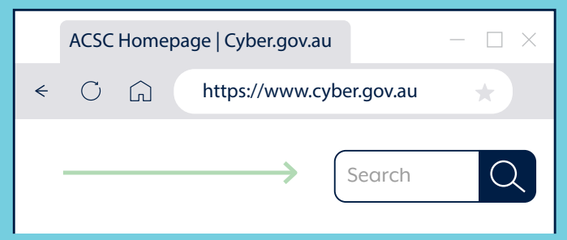
Sugerencia 1: Actualice su dispositivo

La actualización de su software es como el servicio de su coche. Mejora el rendimiento y lo torna más seguro.

Los ciberdelincuentes siempre están buscando formas nuevas de piratear los dispositivos. La selección de actualizaciones automáticas puede corregir cualquier debilidad del software y contener a los piratas.

Para obtener más información, busque "Updates" en cyber.gov.au.





¿LO SABÍA?
Las actualizaciones también pueden agregar nuevas funciones al dispositivo y hacerlo funcionar más rápido.

Sugerencia 2: Active la autenticación multifactorial

La autenticación multifactorial de su cuenta es como una persiana de seguridad para la casa.
Le protege de los delincuentes que intentan entrar.

Cuando la autenticación multifactorial está activada, hay que dar varios datos para acceder a la cuenta. Por ejemplo, es posible que, para ingresar a su perfil de medios sociales, tenga que introducir su contraseña y un código que le llegará por mensaje de texto.

Cuando hay capas múltiples, los ciberdelincuentes tienen más dificultades para conseguir acceso. Puede que descifren una parte, como la contraseña, pero todavía tendrán que obtener otras piezas del rompecabezas para acceder a la cuenta.

Para obtener más información, busque "Multi-factor authentication" o "MFA" en cyber.gov.au

RECUERDE:

Si necesita ayuda para activar la autenticación multifactorial, pídale asistencia a un/a amigo/a o pariente.

Sugerencia 3: Haga una copia de seguridad de su dispositivo

Las "copias de seguridad" son copias de nuestros archivos importantes que ponemos en un sitio seguro. Es como fotocopiar fotos importantes para mantenerlas seguras en caso de perder los originales.

Cuando hacemos una copia de seguridad de la computadora, el teléfono o tableta, las copias de los archivos se guardan en línea o a un dispositivo separado. La copia de seguridad de sus archivos importantes y fotos preciadas le dará tranquilidad.

Si algo le sucede a su dispositivo o si los ciberdelincuentes le atacan, podrá restablecer sus archivos fácilmente a partir de la copia de seguridad.

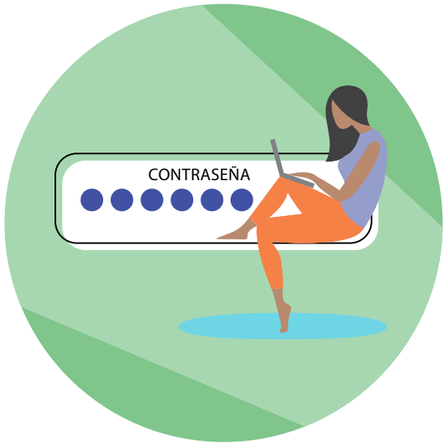
Para obtener más información, busque "Backups" en cyber.gov.au

¿LO SABÍA?

Hacer copias de seguridad periódicamente significa que siempre tendrá acceso a sus archivos más actualizados.

Sugerencia 4: Use una frase de contraseña

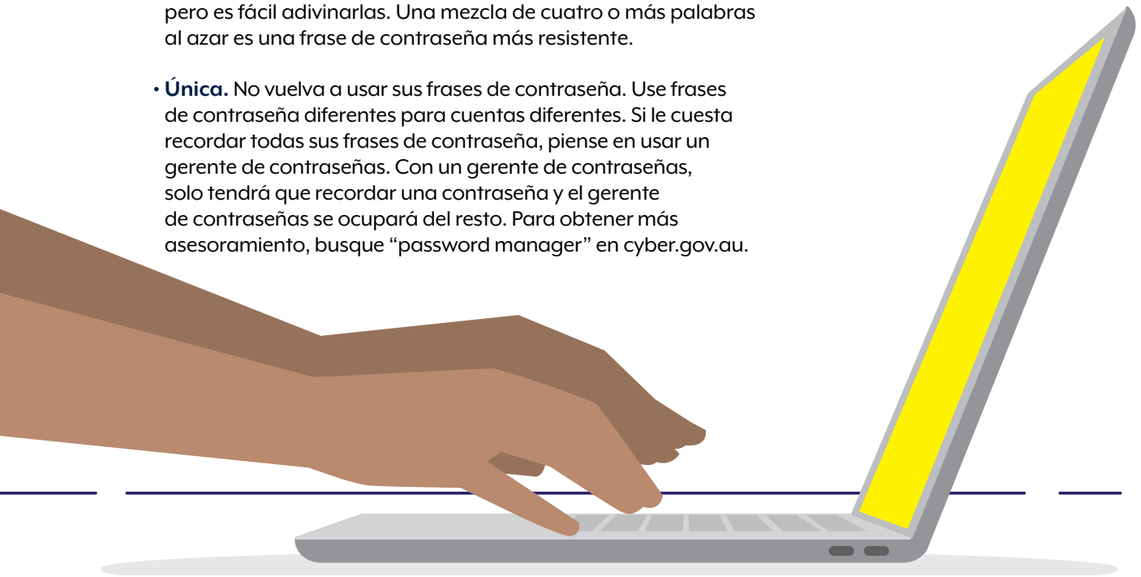
Si una contraseña le pone un candado a su cuenta, ¡una frase de contraseña le da su propio sistema de seguridad! Son versiones más resistentes y seguras de las contraseñas.



Si no puede activar la autenticación multifactorial, use una frase de contraseña para asegurar su cuenta. Las frases de contraseña usan cuatro o más palabras al azar como contraseña. Los ciberdelincuentes tienen dificultades en adivinarlas, pero usted las recordará fácilmente.

Cuando vaya a crear una frase de contraseña, asegúrese de que sea:

- **Larga.** Cuanto más larga, mejor. Use por lo menos 14 caracteres. Lo ideal es usar cuatro o más palabras al azar que pueda recordar. Por ejemplo, "violeta pato papa bote".
- **Imprevisible.** Cuanto menos previsible su frase de contraseña, mejor. Las frases pueden ser frases de contraseña fantásticas, pero es fácil adivinarlas. Una mezcla de cuatro o más palabras al azar es una frase de contraseña más resistente.
- **Única.** No vuelva a usar sus frases de contraseña. Use frases de contraseña diferentes para cuentas diferentes. Si le cuesta recordar todas sus frases de contraseña, piense en usar un gerente de contraseñas. Con un gerente de contraseñas, solo tendrá que recordar una contraseña y el gerente de contraseñas se ocupará del resto. Para obtener más asesoramiento, busque "password manager" en cyber.gov.au.



Para informarse más acerca de la creación de frases de contraseña seguras, busque "Passphrases" en cyber.gov.au

La seguridad en Internet

Sugerencia 5: Reconozca y denuncie las estafas

¿LO SABÍA?

Los ciberdelincuentes son astutos y podrían usar un nombre y dirección electrónica conocidos. Sea cauteloso si:
- **le piden que pague una cuenta urgentemente**
- **le piden que cambie sus datos o contraseña**
- **le piden que haga clic en un enlace o que abra un archivo adjunto.**

Cuanto antes denuncie una estafa, más rápido podremos actuar.

Si usted considera que una persona está intentando usar internet para estafarle, es mejor tomar la iniciativa y ser cauteloso, que arriesgarse a que se aprovechen de usted.

Si parece demasiado bueno para ser verdad, posiblemente lo sea. Si bien un mensaje puede decir que usted ganó un premio o que su computadora tiene un virus, ese mensaje no está dirigido sólo a usted.

Puede que venga de un estafador que quiere aprovecharse de usted. Recuerde, los estafadores suelen fingir que son una persona u organización de confianza. Sospeche si recibe un mensaje que parece venir de una persona de confianza pero usando un nuevo número de teléfono, dirección electrónica o perfil de medios sociales. Antes de responder, verifique que la persona u organización que le envía el mensaje es realmente quien dice ser: póngase en contacto con ella por un canal del que usted puede depender. Por ejemplo, si recibe un mensaje de texto que parece venir de uno de sus hijos, pero viene de un número nuevo, no responda. Envíele primero un mensaje por los medios sociales para comprobar que realmente ha cambiado su número de teléfono.

Conclusión

Ahora que está armado con los conocimientos para usar internet de forma más segura, podrá explorar con confianza y continuar disfrutando del tiempo que pasa en línea.

Pero recuerde, los ciberdelincuentes siempre están inventando nuevas maneras de atacar al público.

No le hace daño a nadie actualizar sus conocimientos de ciberseguridad de vez en cuando y aprender nuevos métodos para mantener la seguridad.

Sugerencias adicionales

¿Quiere aprender más maneras de mantener la seguridad en línea? Vea las sugerencias siguientes.

Piense en lo que está publicando.

Reflexione cuidadosamente acerca de la información que comparte en línea y quién la verá. Sólo acepte peticiones de amistad de personas que conoce en la vida real.

Reciba alertas sobre nuevos peligros.

Inscríbase en nuestro servicio de alerta gratis. Le informará cada vez que encontremos un nuevo peligro cibernético.

También le brindará asesoramiento sobre qué hacer en caso de ataque.

Converse sobre la ciberseguridad con sus familiares y amigos.

Ahora que tiene más conocimientos sobre la ciberseguridad, comparta lo que aprendió con su familia y amigos. Sus conocimientos les ayudarán a evitar las situaciones difíciles en el futuro.

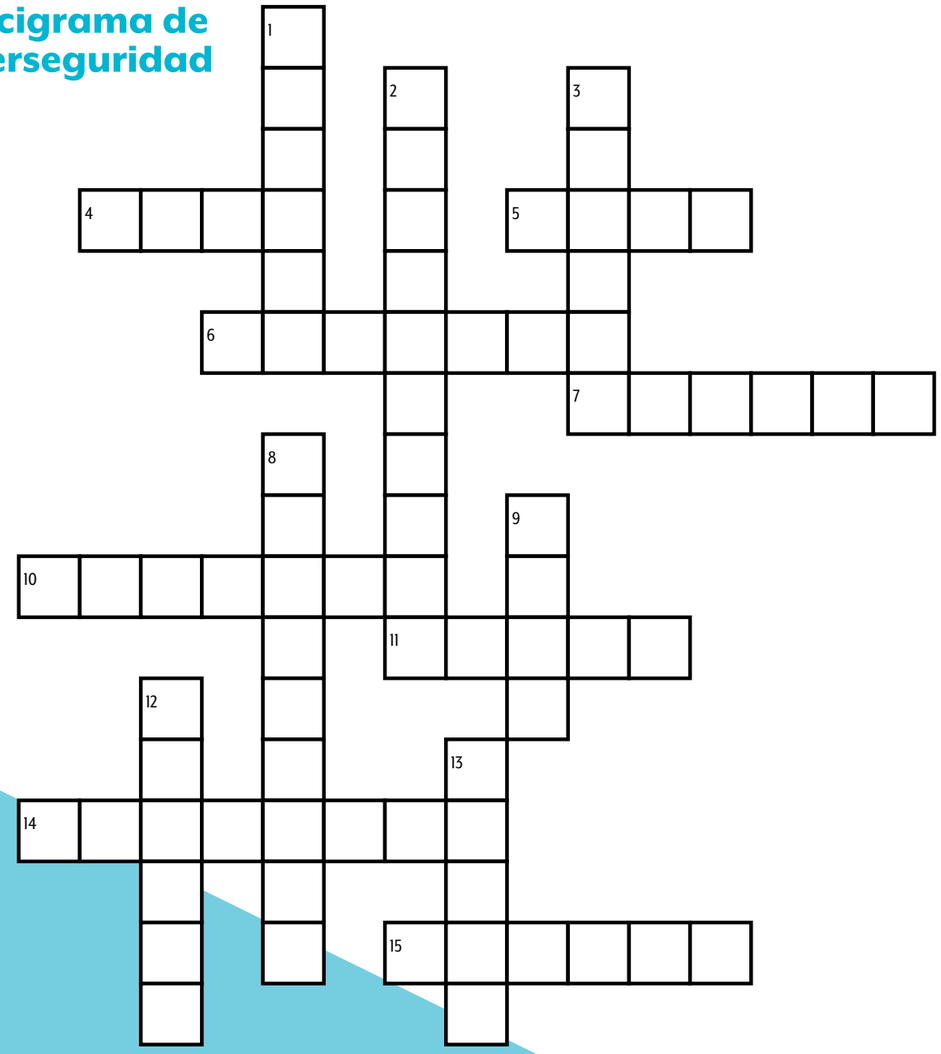
Evite el Wifi público cuando se conecte con su banco o haga compras en línea

El Wifi público es fantástico para mirar videos o leer páginas web, pero reserve todas las actividades que incluyan dinero para la conexión a internet de su casa. El Wifi público puede ser un riesgo.

Denuncie los ciberataques e incidentes para mantener a Australia segura.

Si piensa que ha sido víctima de un ciberdelito, actúe rápidamente. Encontrará más asesoramiento en cyber.gov.au

Crucigrama de ciberseguridad



VERTICALES

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

HORIZONTALES

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Guías suplementarias

Para obtener más información consulte la serie *La ciberseguridad personal*: tres guías preparadas para ayudar a todos los australianos a comprender los fundamentos de la ciberseguridad y las medidas que pueden tomar para protegerse de los peligros cibernéticos comunes.

Para acceder a las tres guías vaya a **cyber.gov.au**

Respuestas al crucigrama

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Notas

Para obtener más información o denunciar un incidente de ciberseguridad contáctenos:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Este número es para llamadas en Australia únicamente.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre