



**Actúe ya mismo.
Manténgase a salvo.**

actnowstaysecure.gov.au

¿Qué está arriesgando en línea?

A medida que la tecnología avanza a paso acelerado y pasamos más tiempo conectados en línea, los australianos seguimos siendo vulnerables a los ciberataques.

La campaña «Actúe ya mismo. Manténgase a salvo» informa a los australianos sobre medidas simples de ciberseguridad que todos podemos tomar para protegernos en línea.

Actúe ya mismo. Manténgase a salvo.

Cómo mantener la seguridad en línea

Use una frase de contraseña única y fuerte para cada cuenta

El uso de una frase de contraseña única y fuerte para cada una de sus cuentas en línea es una de las medidas más eficaces que puede tomar para mantenerse a salvo en línea.

Las frases de contraseña son contraseñas más seguras. Contienen una secuencia de palabras al azar. Usted las puede recordar más fácilmente, pero a los ciberdelincuentes les resulta más difícil adivinarlas.

Para que sus frases de contraseña sean fuertes y únicas, deberán:

- ✓ tener cuatro o más palabras al azar
- ✓ contener 15 o más caracteres
- ✓ ser diferentes para cada cuenta
- ✓ no incluir información que permita la identificación, como nombres de la familia, fechas de cumpleaños o direcciones
- ✓ incluir símbolos, mayúsculas o números, si el sitio web o servicio lo requieren.

Piense en usar un gerente de contraseñas que cree y guarde sus frases de contraseña únicas.

Instale todas las actualizaciones de software para mantener la seguridad de sus dispositivos

Para mantenerse a salvo en línea es de importancia crítica que instale siempre las actualizaciones de software para todos sus dispositivos conectados a internet (como el celular, la computadora portátil o el reloj inteligente).

Las actualizaciones de software corrigen las debilidades o brechas de seguridad de los dispositivos. La instalación de actualizaciones periódicas mantendrá sus dispositivos a salvo y los ciberdelincuentes tendrán más dificultades para conseguir acceso a ellos.

Active las actualizaciones automáticas e instálelas cuando reciba las instrucciones para hacerlo.

Configure siempre la autenticación multifactorial

Active la autenticación multifactorial cuando esta esté disponible para añadir una capa extra de seguridad a todas sus cuentas en línea.

La autenticación multifactorial requiere dos o más métodos de verificación para conectarse a su cuenta. Por ejemplo, después de introducir su contraseña o frase de contraseña, se le pedirá que proceda a una segunda verificación como introducir un código que se le envió por medio de una aplicación de autenticación, por e-mail o mensaje de texto.

La autenticación multifactorial protege su cuenta incluso si uno de sus otros métodos de autenticación (como una frase de contraseña) ha quedado expuesto.



**Actúe ya mismo.
Manténgase a salvo.**

actnowstaysecure.gov.au

¿Quiere más maneras de mantener la seguridad en línea?

¿Está buscando más maneras de mantener la ciberseguridad? He aquí algunas otras medidas que puede tomar para protegerse en línea.

Sea prudente cuando use Wi-fi público

Cuando esté usando Wi-fi público la conexión no es segura y, por lo tanto, no acceda a información confidencial o privada como redes sociales, correo electrónico o transacciones bancarias en línea. Los ciberdelincuentes podrían acceder a toda información que usted introduzca.

Revise y actualice regularmente sus configuraciones de privacidad y ubicación

Es importante revisar las configuraciones de privacidad y ubicación con frecuencia para asegurarse de no estar compartiendo accidentalmente con el público información personal o que le identifique.

Compruebe las configuraciones siguientes: configuraciones de privacidad de sus cuentas de redes sociales y de rastreo de geolocalización de sus aplicaciones y dispositivos.

Converse con amigos y parientes acerca de cómo mantener la ciberseguridad

La información y concientización son de importancia crítica para mantener la seguridad en línea de usted, su familia y sus amigos, especialmente si comparten dispositivos conectados con internet. Hablar de esta cuestión con sus allegados mantiene la prioridad máxima de la ciberseguridad y garantiza que estén recibiendo la información más reciente sobre cómo protegerse en línea.

Aprenda a detectar estafas

Los estafadores engañan a la gente y les convencen de darles dinero o de revelar información personal.

Nunca le dé dinero o información personal a nadie a menos que usted tenga la certeza de saber con quién está tratando. Para comprobarlo, póngase en contacto con la persona u organización y para ello utilice los datos que usted haya encontrado en una página web o aplicación oficial.

Denuncie los ciberataques e incidentes

La denuncia de estafas o ciberincidentes es de importancia crítica pues ayuda al gobierno a detectar las nuevas tendencias, alertar a la comunidad y ayudar en la recuperación de un incidente cibernético.

Aprenda los pasos sencillos para protegerse en actnowstaysecure.gov.au



**Actúe ya mismo.
Manténgase a salvo.**

actnowstaysecure.gov.au