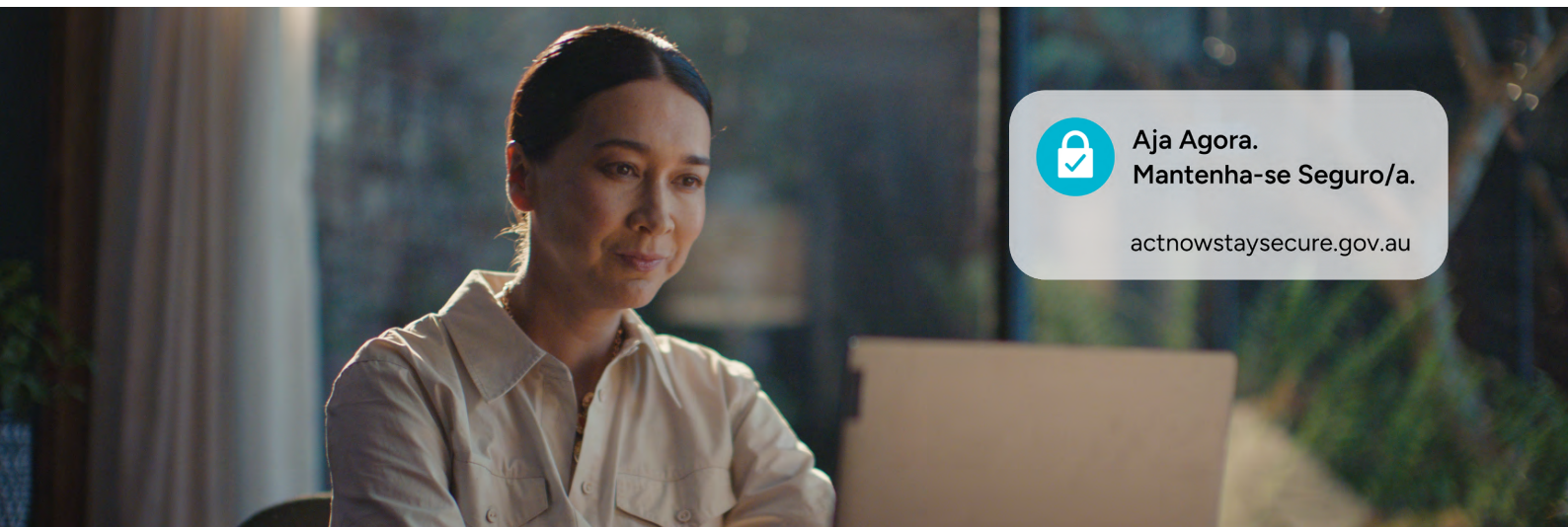




Aja Agora.
Mantenha-se Seguro/a.

actnowstaysecure.gov.au

O que está a arriscar online?

Os australianos continuam a estar vulneráveis a ataques cibernéticos, à medida que a tecnologia avança rapidamente, e porque passam mais tempo online.

A campanha Aja Agora. Mantenha-se Seguro/a. está a educar os australianos sobre simples ações de segurança cibernética que todos podem tomar para se proteger online.

Aja Agora. Mantenha-se Seguro/a.

Como estar seguro/a online

Use uma frase-passe única e forte para cada conta

Uma das ações mais eficazes que pode tomar para se manter seguro online, é usar uma frase-passe única e forte para cada uma das suas contas online.

Uma frase-passe é uma palavra-passe mais segura. Contém uma sequência de palavras aleatórias. São mais fáceis de lembrar, mas mais difíceis de adivinhar para os cibercriminosos.

Para ser forte e única, a sua frase-passe deve:

- ✓ ter quatro ou mais palavras aleatórias
- ✓ conter 15 ou mais caracteres
- ✓ ser diferente para cada conta
- ✓ não incluir informação pessoal tal como apelidos, datas de nascimento ou moradas
- ✓ incluir símbolos, letras maiúsculas ou números, caso seja exigido pelo site ou serviço.

Considere usar um gestor de palavras-passe para criar e armazenar as suas frases-passe únicas.

Instale todas as atualizações de software para manter os seus dispositivos seguros

É fundamental que instale sempre as atualizações de software em todos os seus dispositivos ligados à Internet (tal como telemóveis, computadores portáteis ou relógios inteligentes) para se manter seguro/a online.

As atualizações de software corrigem vulnerabilidades ou falhas na segurança dos seus dispositivos. Instalar atualizações regularmente mantém os seus dispositivos seguros e torna mais difícil para cibercriminosos os acederem.

Ative as atualizações automáticas e instale-as sempre que lhe for solicitado.

Configure sempre a autenticação multifator

Ative a autenticação multifator sempre que disponível para adicionar uma camada extra de segurança a todas as suas contas online.

A autenticação multifator requer dois ou mais métodos de verificação para aceder à sua conta. Por exemplo, depois de inserir a sua palavra-passe ou frase-passe, será solicitado/a a fornecer uma segunda verificação, como inserir um código enviado via app autenticadora, e-mail ou mensagem de texto.

A autenticação multifator protege a sua conta mesmo se um dos seus métodos de autenticação (como uma frase-passe) seja comprometido.



Aja Agora.
Mantenha-se Seguro/a.

actnowstaysecure.gov.au

Quer mais formas de estar seguro online?

Procura mais formas de se manter seguro/a online? Eis outras ações que pode tomar para se proteger online.

Tenha cautela ao utilizar Wi-Fi público

Quando utilizar Wi-Fi público, não aceda a informação sensível ou privada, pois a ligação não é segura. Isto inclui redes sociais, e-mail ou bancos online. Qualquer informação que inserir poderá ser acedida por cibercriminosos.

Verifique e atualize regularmente as suas configurações de privacidade e localização

É importante verificar frequentemente as suas configurações de privacidade e localização para garantir que não está a partilhar acidentalmente a sua informação pessoal ou identificadora com o público.

As configurações a verificar incluem as configurações de privacidade das suas contas de redes sociais e o rastreamento de geolocalização nos seus aplicativos e dispositivos.

Fale sobre como estar seguro/a ciberneticamente com amigos e família

A educação e a sensibilização são essenciais para se manter seguro/a online, bem como a sua família e amigos – especialmente se partilha dispositivos ligados à Internet. Falar sobre segurança cibernética com a sua rede de contatos mantém o tema em mente e garante que estão a receber a informação mais recente sobre como se proteger online.

Aprenda a identificar fraude

Os golpistas enganam as pessoas para que paguem dinheiro ou forneçam informações pessoais.

Nunca envie dinheiro ou informação pessoal a ninguém se não tiver a certeza de com quem está a lidar. Verifique a identidade através de entrar em contacto com a pessoa ou organização usando detalhes que pode encontrar num site ou aplicativo oficial.

Reporte ataques cibernéticos e incidentes

Denunciar golpes ou incidentes cibernéticos é fundamental para ajudar o governo a identificar novas tendências, alertar a comunidade e ajudá-lo/a na recuperação após o incidente cibernético.

Aprenda passos simples para se proteger em actnowstaysecure.gov.au



Aja Agora.
Mantenha-se Seguro/a.

actnowstaysecure.gov.au