



Australian Government



Aja Agora.
Mantenha-se Seguro/a.

Como você pode se manter seguro online

Versão em Leitura Fácil



Como usar este guia



Nós somos o Governo Australiano.

Nós escrevemos este guia.



Nós escrevemos algumas palavras em **negrito**.

Nós explicamos o que essas palavras significam.

Também há uma lista dessas palavras na página 28.



Você pode pedir apoio a alguém de confiança para:

- ler este guia
- encontrar mais informações.



Este é um resumo em Leitura Fácil de outro guia.

Ele inclui apenas as ideias mais importantes.



Você pode encontrar o outro guia em nosso site.

www.actnowstaysecure.gov.au

O que há neste guia?

Sobre este guia	4
Mantenha suas contas seguras	6
Verifique suas configurações para proteger suas informações	10
Proteja seus dispositivos	16
Golpes	20
Fale	25
Lista de palavras	28
Fale conosco	30

Sobre este guia



Todos nós precisamos pensar em como podemos nos manter seguros online.

Chamamos isso de segurança **cibernética**.



Cibernético significa algo relacionado à internet.



Este guia explica algumas coisas que você pode fazer para se proteger online.

Por exemplo, contra **crimes cibernéticos**.



Crime cibernético é quando criminosos usam a internet para cometer crimes.

Por exemplo, eles podem usar a internet para:

- roubar suas informações pessoais
- assumir suas contas ou perfis online.

O crime cibernético pode acontecer em qualquer dispositivo.



Isso inclui:

- seu computador
- seu smartphone
- seu smartwatch.



Há coisas que você pode fazer para se manter seguro contra crimes cibernéticos.



Nós explicamos o que você pode fazer nas páginas seguintes.

Mantenha suas contas seguras



Você deve pensar em como pode manter suas contas online seguras.

Use frases-senha fortes e diferentes



Uma **frase-senha** é um tipo mais forte de senha.
É muito difícil para outras pessoas adivinharem.



Usar frases-senha fortes e diferentes é uma das melhores maneiras de proteger suas contas.



Você deve usar uma frase-senha diferente para cada uma das suas contas online.



Frases-senha fortes incluem:

- 4 ou mais palavras aleatórias
- 15 ou mais letras e números.



Você pode incluir algumas letras maiúsculas.



Você também pode usar símbolos como:

- um hífen
- símbolo de dólar
- símbolo de email @.



Você não deve usar nenhuma informação pessoal em suas frases-senha.



Por exemplo:

- sua data de nascimento
- os nomes dos seus familiares ou animais de estimação.

Adicione etapas extras para entrar em suas contas



Você pode proteger suas contas online com **autenticação multifator (MFA)**.

MFA é quando você usa 2 ou mais formas diferentes para entrar na sua conta todas as vezes.



Por exemplo, você pode precisar digitar sua frase-senha primeiro.

Depois, você digita um código que recebe no seu celular.

Você pode ter a opção de:



- obter um aplicativo no seu celular para gerar o código



- receber o código por email



- receber o código por mensagem de texto.



A MFA torna mais difícil para outras pessoas acessarem suas contas online.

Mesmo que descubram sua frase-senha.

Verifique suas configurações para proteger suas informações



Você pode verificar se suas configurações estão protegendo suas informações online.



Isso inclui configurações em:

- suas contas online
- seus dispositivos
- seus aplicativos.



Você pode:

- alterar suas configurações
- escolher quais aplicativos podem usar suas informações.

Você pode encontrar as configurações no seu dispositivo:



- procurando o ícone de engrenagem
ou
- digitando “configurações” na barra de pesquisa do seu dispositivo.



Você pode encontrar configurações em um aplicativo ou conta online abrindo o menu.

O menu geralmente se parece com 3 linhas retas.

Algumas dessas configurações podem compartilhar informações sobre:



- quem você é
- onde você está
- onde você mora.



Compartilhar essas informações online pode colocar você em risco de crimes cibernéticos.



Criminosos cibernéticos podem usar suas informações para fingir ser você.

Por exemplo, eles podem usar informações como:



- onde você mora



- os nomes dos seus familiares



- os nomes dos seus animais de estimação.



Você pode configurar suas contas para que apenas pessoas que você conhece possam ver seus perfis em redes sociais.

Por exemplo, seu perfil no Facebook.



Essas configurações geralmente são chamadas de configurações de privacidade.



Você também pode controlar suas **configurações de localização**.

As configurações de localização mostram onde seu dispositivo está.



Você pode ativar ou desativar as configurações de localização.

Você também pode escolher quais aplicativos podem usar suas configurações de localização.



Você pode fazer isso para:

- suas contas online
- seus dispositivos
- seus aplicativos.

Alguns aplicativos também podem pedir para:



- usar sua câmera



- ver suas fotos.



Você só deve permitir que aplicativos que você conhece usem sua câmera e suas fotos.

Proteja seus dispositivos



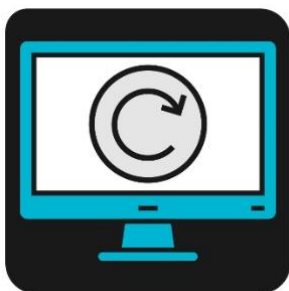
Você deve pensar em como pode proteger seus dispositivos para ajudar a se manter seguro online.

Por exemplo, seu celular ou smartwatch.



Isso é importante para dispositivos que se conectam à internet.

Atualize seus dispositivos



Você pode atualizar seus dispositivos para mantê-los seguros online.

Por exemplo, seu celular e notebook.



Seu dispositivo pode chamar isso de atualização de software.



As atualizações ajudam o dispositivo a se proteger contra crimes cibernéticos.



Você pode configurar um dispositivo para atualizar automaticamente.



Você pode aprender mais sobre como atualizar seus dispositivos em nosso site.

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

Redes Wi-Fi públicas



Você deve ter cuidado ao usar **Wi-Fi público**.



Wi-Fi público é internet sem fio gratuita que você pode usar em locais públicos.



Por exemplo, em:

- um café
- aeroporto
- hotel.



Você deve ter cuidado com as informações que digita em um site usando Wi-Fi público.



Por exemplo:

- seus dados bancários
- suas contas de email
- seus perfis em redes sociais.



Alguns criminosos cibernéticos podem usar Wi-Fi público para:

- ver o que você está fazendo online
- roubar suas informações.

Isso acontece porque:



- qualquer pessoa pode usar



- é mais difícil proteger seus dispositivos.



Você pode aprender como se manter seguro usando Wi-Fi público em nosso site.

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

Golpes



Chamamos de **golpe** quando alguém tenta:

- enganar você
- roubar seu dinheiro.



Um **golpista** é alguém que aplica golpes.

Golpistas podem tentar enganar você por meio de:



- mensagem de texto ou ligação
- email
- redes sociais
- um site.



Eles podem parecer amigáveis.

Mas podem enganar você para que você forneça suas informações.

Eles podem usar isso para:



- acessar suas contas online



- fingir ser você



- roubar seu dinheiro.

Golpistas também podem:



- criar contas falsas para enganar você



- compartilhar links e anúncios para você clicar.

Como identificar um golpe

Pode ser um golpe se:



- pedir que você faça algo rapidamente



- oferecer muito dinheiro



- pedir dinheiro



- pedir que você clique em um link.



Golpistas também podem fingir ser uma organização que você conhece e confia.

Por exemplo, seu banco.



Golpistas fazem isso para que você compartilhe suas informações pessoais com eles.



Você deve parar de falar com a pessoa se achar que ela é um golpista.



Você deve verificar se a pessoa é quem diz ser.

Você pode entrar em contato com a pessoa ou organização usando informações confiáveis que você mesmo encontrou.



Aja rapidamente para se proteger se algo parecer errado.

Denunciar um golpe



O Scamwatch ajuda os australianos a:

- entender golpes
- denunciar golpes.



O Scamwatch também ajuda australianos que sofreram golpes.



Você pode denunciar um golpe no site do Scamwatch.

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

Fale



Você deve falar abertamente sobre como as pessoas podem se proteger online.

Isso inclui:



- denunciar crimes cibernéticos



- compartilhar o que você sabe com familiares e amigos.



Vamos explicar como você pode falar nas próximas páginas.

Denuncie crime cibernético

Denunciar crimes cibernéticos ajuda o governo a:



- entender como criminosos cibernéticos tentam atacar as pessoas



- proteger mais pessoas.



Você pode denunciar crimes cibernéticos no site ReportCyber.

www.cyber.gov.au/report

Converse com sua família e amigos sobre segurança online



Você deve compartilhar suas dicas sobre como se manter seguro online com sua família e amigos.

Você também pode aprender com eles.



Você pode proteger a si mesmo e as pessoas ao seu redor compartilhando o que sabe sobre segurança online.



Isso também é importante se você compartilha dispositivos com outras pessoas.

Lista de palavras

Esta lista explica o que significam as palavras em **negrito** neste guia.



Cibernético

Cibernético significa algo relacionado à internet.



Crime cibernético

Crime cibernético é quando criminosos usam a internet para cometer crimes.

Por exemplo, eles podem usar a internet para:

- roubar suas informações pessoais
- assumir suas contas online.



Configurações de localização

Configurações de localização mostram onde seu dispositivo está.



Autenticação multifator (MFA)

MFA é quando você usa 2 ou mais formas diferentes para entrar na sua conta todas as vezes.



Frase-senha

Uma frase-senha é um tipo mais forte de senha. É muito difícil para outras pessoas adivinharem.



Wi-Fi público

Wi-Fi público é internet sem fio gratuita que você pode usar em locais públicos.



Golpes

Chamamos de golpe quando alguém tenta:

- enganar você
- roubar seu dinheiro.



Golpistas

Um golpista é alguém que aplica golpes.

Fale conosco



Você pode ligar para a Linha Direta de Segurança Cibernética da Austrália.

1300 292 371



Você pode visitar nosso site.

www.actnowstaysecure.gov.au



Você pode denunciar crimes cibernéticos no site ReportCyber.

www.cyber.gov.au/report



O Information Access Group criou este documento em Leitura Fácil usando fotografias de banco de imagens e imagens personalizadas. As imagens não podem ser reutilizadas sem permissão. Para quaisquer dúvidas sobre as imagens, visite www.informationaccessgroup.com. Informe o número do projeto 6342.
