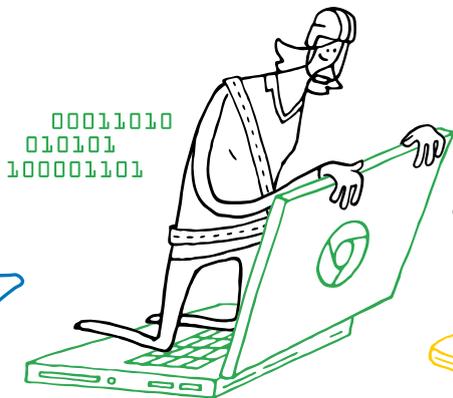


# É Bom Saber

Um guia para se manter  
seguro e protegido online



Google™

# Índice

1. Como pode permanecer seguro e protegido online.
2. Como pode proteger a sua família online.
3. Saber como a Google o(a) ajuda a proteger-se.

## De que se trata?

A campanha É Bom Saber da Google tem como objetivo ajudá-lo(a) a si e à sua família e amigos a manterem-se seguros e protegidos na Internet.

Este folheto contém dicas e sugestões úteis que são fáceis de memorizar e de pôr em prática. Incluímos autocolantes com alguns dos principais conselhos, para que os possa colocar no computador ou bloco de notas e utilizá-los como lembretes úteis.

Para obter informações mais detalhadas acerca dos tópicos que constam neste folheto e muito mais, aceda ao Website É Bom Saber

[www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)



# 1. Como pode permanecer seguro e protegido online

A Internet oferece muitas oportunidades para explorar, criar e colaborar. Mas é importante manter-se seguro e protegido, para que possa aproveitar ao máximo.

Existem vários tipos diferentes de cibercrime. Um criminoso pode tentar obter acesso às suas informações, como a palavra-passe do seu email, detalhes bancários ou o número da segurança social.

Um criminoso também pode tentar utilizar a Internet para o enganar, vender-lhe produtos falsificados ou levá-lo a fazer coisas que custam dinheiro. Por outro lado, tal como um ladrão que rouba um carro de fuga sem se importar quem é o dono, podem pretender utilizar o seu computador ou um Website que possui como ferramenta para cometer cibercrimes.

Quer seja um utilizador da Internet principiante ou um especialista, as sugestões e ferramentas aqui apresentadas para o ajudar a navegar na Web de forma segura e protegida são sempre úteis de saber.

## Proteger as suas palavras-passe

As palavras-passe são a primeira linha de defesa contra cibercriminosos. É crucial escolher palavras-passe fortes diferentes para cada uma das suas contas importantes e é uma boa prática atualizar as suas palavras-passe regularmente. Siga estas sugestões para criar palavras-passe fortes e mantê-las protegidas.

1. Utilize uma palavra-passe exclusiva para cada uma das suas contas importantes, como as contas de email e do banco online.
2. Utilize uma palavra-passe comprida, composta por números, letras e símbolos.
3. Muitos serviços irão enviar-lhe um email para um endereço de email de recuperação se tiver de repor a sua palavra-passe; logo, certifique-se de que o seu endereço de email de recuperação está atualizado e é uma conta à qual ainda consegue aceder.

Por exemplo, pense numa expressão que mais ninguém saiba e relacione-a com esse Website em particular, para ser mais fácil de memorizar. Para o seu email, pode começar com "Os meus amigos Carlos e Jasmim enviam-me um email engraçado por dia" e depois utilize números e letras para a recriar: "OmaC&Je1eepd" é uma palavra-passe com muitas variações. Depois, repita este processo para outros sites.

OmaC&Je1eepd



## Evitar o roubo de identidade

Tal como não daria a um assaltante a chave de sua casa, certifique-se de que se protege contra fraudes e roubo de identidade online. Conheça os truques habituais que os criminosos utilizam, para poder proteger-se contra fraudes e roubo de identidade online. Aqui estão algumas sugestões simples.

1. Não responda se vir um email, mensagem instantânea ou página Web suspeita a pedir as suas informações pessoais ou financeiras.
2. Nunca introduza a sua palavra-passe, caso tenha chegado a um site através de um link num email ou chat em que não confia.
3. Não envie a sua palavra-passe por email e não a partilhe com outras pessoas.

Se vir uma mensagem de alguém que conhece que não pareça ser habitual dessa pessoa, a sua conta poderá ter sido comprometida por um cibercriminoso que está a tentar obter dinheiro ou informações suas. Deste modo, tenha cuidado com a forma como responde. As táticas mais frequentes incluem pedir-lhe que envie dinheiro com urgência, a pessoa afirmar que está presa noutro país ou que o telefone dela foi roubado, pelo que não pode ser contactada. A mensagem também poderá pedir-lhe que clique num link para ver uma imagem, um artigo ou um vídeo, o qual, na verdade, o(a) direciona para um site que poderá roubar as suas informações. Pense bem antes de clicar!

# Evitar esquemas fraudulentos

Não, provavelmente não ganhou a lotaria. Não consegue ganhar tanto dinheiro assim a trabalhar a partir de casa. E esse negócio poderá realmente ser bom demais para ser verdade.

A Web pode ser um lugar fantástico, mas nem todas as pessoas online têm boas intenções. Eis três formas simples de evitar falsários e permanecer seguro na Web:

- 1. Cuidado com estranhos com presentes.** Se alguém lhe diz que é um vencedor e lhe pede para preencher um formulário com as suas informações pessoais, não se sinta tentado a começar a preenchê-lo. Mesmo que não carregue em “Enviar”, ainda pode estar a enviar as suas informações a falsários caso tenha começado a introduzir os seus dados nos formulários.
- 2. Faça a sua pesquisa.** Quando fizer compras online, faça pesquisas sobre o vendedor e desconfie de preços questionavelmente baixos, tal como faria se estivesse a comprar algo numa loja local. Examine negócios online que parecem ser bons demais para ser verdade. Ninguém gosta de ser enganado e comprar artigos falsificados.
- 3. Em caso de dúvida, jogue pelo seguro.** Tem um mau pressentimento acerca de um anúncio ou oferta? Confie nos seus instintos! Clique apenas em anúncios ou compre produtos em sites seguros, analisados e fidedignos.



## Bloquear o ecrã ou dispositivo

Nunca iria sair de casa durante o resto do dia e deixar a porta da frente completamente aberta, pois não? O mesmo princípio aplica-se aos dispositivos que utiliza. Deve sempre bloquear o seu ecrã quando terminar de utilizar o computador, portátil ou telemóvel.



Para obter uma maior segurança, também deve definir o seu dispositivo para bloquear automaticamente quando este entra no modo de suspensão. Isto é especialmente importante para telemóveis ou tablets, pois é mais provável que sejam colocados no local errado e descobertos por pessoas que não quer que acedam à sua informação, assim como computadores de casa que se encontram em espaços partilhados.

## Utilizar redes seguras

É bom ter um cuidado adicional sempre que ficar online utilizando uma rede que não conhece ou na qual não confia, tal como o Wi-Fi gratuito no seu café local. O fornecedor de serviços pode monitorizar todo o tráfego na rede dele, o que pode incluir os seus dados pessoais.

Quando se liga através de uma rede Wi-Fi pública, qualquer pessoa nas redondezas pode monitorizar as informações que são transmitidas entre o seu computador e a zona Wi-Fi se a sua ligação não estiver encriptada. Evite efetuar atividades importantes como ir ao Website do banco ou fazer compras através de redes públicas.

Se utilizar o Wi-Fi em casa, deve certificar-se de que utiliza uma palavra-passe para proteger o seu router. Siga as instruções fornecidas pelo seu Fornecedor de Serviços de Internet ou pelo fabricante do router para definir a sua própria palavra-passe para o router, em vez de utilizar a palavra-passe predefinida, que poderá ser do conhecimento dos criminosos. Se os criminosos conseguirem aceder ao seu router, podem alterar as suas definições e espiar a sua atividade online.

Finalmente, também deve certificar-se de que protege a sua rede Wi-Fi de casa, para que outras pessoas não a possam utilizar, de forma a obter uma camada adicional de segurança. Isto significa a configuração de uma palavra-passe para proteger a sua rede Wi-Fi e, tal como com outras palavras-passe que escolhe, certifique-se de que opta por uma mistura exclusiva de números, letras e símbolos para que outros não possam facilmente adivinhar a sua palavra-passe. Deve escolher a definição WPA2 quando configurar a sua rede, para obter uma proteção mais avançada.

# Conhecer as ferramentas de segurança e privacidade da Google

Com a Google, tem várias ferramentas que podem ajudar a mantê-lo(a) seguro(a) e a manter as suas informações privadas e seguras. Eis algumas das nossas ferramentas mais populares que ajudam a fazer com que o Google funcione melhor para si.

## Confirmação em Dois Passos

Para a sua Conta Google ter níveis de proteção ainda mais fortes, oferecemos a confirmação em dois passos aos nossos utilizadores. Esta ferramenta adiciona uma camada extra de segurança, exigindo não apenas uma palavra-passe, mas também um código de confirmação para iniciar sessão numa Conta Google. Mesmo que a sua palavra-passe seja decifrada, adivinhada ou roubada, um utilizador mal intencionado não pode iniciar sessão na sua conta sem introduzir o código de confirmação que iremos enviar para o seu telemóvel. Oferecemos a confirmação em dois passos em mais de 50 idiomas e 175 países.

## Definições da Conta Google

Na página de definições de Conta, pode ver serviços e informações associados à sua Conta Google e alterar as suas definições de segurança e privacidade.

## Modo de Navegação Anónima

No modo de navegação anónima, as páginas que abre e os ficheiros que transfere não são gravados no histórico de navegação ou de transferências do Chrome. Também pode utilizar esta funcionalidade no Chrome para Android e o Chrome é agora o navegador predefinido para os novos produtos Android, permitindo-lhe navegar na Web no seu telemóvel ou tablet em privado.



## Painel de controlo do Google

O Painel de controlo do Google mostra-lhe o que está armazenado na sua Conta Google. A partir de uma localização central, pode facilmente visualizar e atualizar as suas definições para serviços como o Blogger, Calendário Google, Google Docs, Gmail, Google+ e muito mais.

## Definições de Anúncios

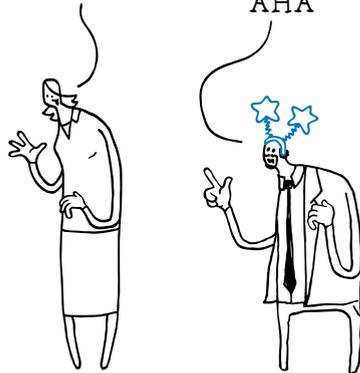
Os anúncios ajudam a financiar muitos dos serviços online gratuitos na Web que adora e utiliza todos os dias. Com as Definições de Anúncios do Google, pode compreender como os anúncios são escolhidos para si, controlar as suas informações utilizadas para selecionar anúncios e bloquear anunciantes específicos.

## Círculos do Google+

Os círculos do Google+ ajudam-no a gerir os seus amigos e contactos. Pode colocar os seus amigos num círculo, a sua família noutro e o seu chefe sozinho num círculo, tal como na vida real. De seguida, pode partilhar conteúdo relevante, como mensagens do Google+, vídeos do YouTube ou Fichas de empresas locais, com as pessoas certas quando quiser.

O MEU PATRÃO É  
TÃO ESTRANHO

ÃHA





## É bom saber. É bom manter.

5 sugestões a reter para ajudá-lo(a) a manter-se seguro(a) e protegido(a) online.

Para obter mais sugestões de segurança, aceda a [www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)



Evite esquemas fraudulentos. Não responda se vir um email, mensagem instantânea ou página Web suspeita a pedir as suas informações pessoais ou financeiras.

Google

[www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)



Confirme habitualmente as suas definições de privacidade e segurança e personalize a forma como pretende partilhar conteúdos.

Google

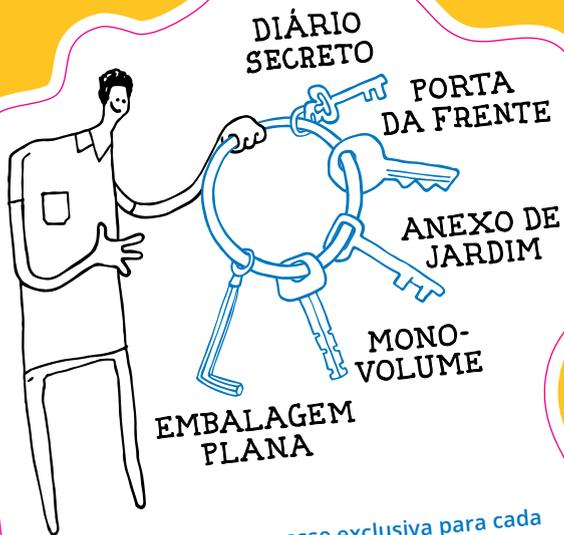
[www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)



Não envie a sua palavra-passe por email e não a partilhe com outros.

Google

[www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)



Utilize uma palavra-passe exclusiva para cada uma das suas contas importantes, como as contas de email e do banco online.



[www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)



[www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)



## 2. Como pode proteger a sua família online

Sabemos até que ponto é importante proteger e educar os jovens sobre o modo de utilizar a Internet e queremos proporcionar uma experiência segura a todos os nossos utilizadores.

No que diz respeito à segurança familiar, o nosso objetivo é:

- Proporcionar a pais e professores ferramentas que os ajudem a escolher o conteúdo que as suas crianças veem online.
- Oferecer sugestões e conselhos às famílias sobre como permanecerem seguras online.
- Trabalhar estreitamente com organizações, como associações de beneficência, outras empresas no nosso ramo e entidades legais dedicadas a proteger os jovens.

# Ferramentas de segurança familiar

Incorporamos nos nossos produtos ferramentas e controlos que ajudam o utilizador a controlar a sua experiência online.

## Google Pesquisa Segura e Bloquear

A Pesquisa Segura foi concebida para filtrar sites com conteúdo sexualmente explícito e removê-los dos resultados de pesquisa. Embora nenhum filtro seja 100% seguro, a Pesquisa Segura ajuda o utilizador a evitar conteúdo que poderá preferir não ver ou que prefere que os seus filhos não encontrem por acaso.

Se lhe preocupa a hipótese de outras pessoas alterarem as definições de Pesquisa Segura sem o seu conhecimento, pode protegê-las com uma palavra-passe usando Bloquear Pesquisa Segura. Uma vez bloqueada, a página de resultados de pesquisa do Google será visivelmente diferente para indicar que a Pesquisa Segura está bloqueada.

Para ativar a Pesquisa Segura, visite a página Preferências de Pesquisa:

**[www.google.pt/preferences](http://www.google.pt/preferences)**

## Controlos de partilha no YouTube

Por vezes, pode querer guardar para si os vídeos da sua família ou partilhá-los apenas com pessoas selecionadas. Poderá fazê-lo no YouTube ao selecionar não listado ou privado quando carrega o vídeo.



### **Modo de Segurança do YouTube e Bloqueio**

O Modo de Segurança dá aos utilizadores a opção de não ver conteúdos para adultos que possam achar ofensivos, mesmo que não estejam contra as nossas Regras da Comunidade. Quando ativa o Modo de Segurança, os vídeos com conteúdos para adultos ou com restrição de idade não aparecem na pesquisa de vídeos.

Para aceder ao Modo de Segurança e ativá-lo, clique em Modo de Segurança na parte inferior de todas as páginas para abrir a definição de preferências.

### **Filtragem de conteúdo para Android**

O Google Play requer que os programadores coloquem uma etiqueta nas suas aplicações de acordo com sistema de classificações do Google Play, que consiste em quatro níveis: para todos, nível de maturidade baixo, nível de maturidade médio ou nível de maturidade alto. Usando um código PIN, os utilizadores podem bloquear uma definição para filtrar aplicações nos seus dispositivos para que só possam ser vistas e transferidas aplicações consideradas apropriadas para a sua utilização.

### **Google+**

Diversas funcionalidades fornecem-lhe transparência e poder de escolha sobre quem pode ver o tipo de informações que publica ou partilha, incluindo círculos que permitem seleccionar exactamente quem vê as suas publicações, definições de notificações que permitem especificar quem o pode contactar e definições de visibilidade que permitem tornar privado o seu perfil.

### **Blogger**

No Blogger, o seu blogue é, por predefinição, público e pode ser lido por qualquer pessoa na Internet. Se pretender torná-lo privado, pode limitar os visitantes do seu blogue apenas às pessoas que opta por convidar.

# Comunicar conteúdo impróprio

Alguns dos nossos produtos, tais como o Google+, o YouTube e o Blogger, proporcionam meios para criar, publicar e partilhar o seu próprio conteúdo. Criámos ferramentas que lhe permitem notificar-nos, caso encontre conteúdo que não deva estar no site. Segue-se um guia rápido sobre como comunicar conteúdo impróprio em alguns dos nossos produtos mais populares.

## Google+

Pode comunicar vários tipos de conteúdo impróprio no Google+; pode comunicar uma publicação ou comentário, um vídeo ou uma fotografia, assim como um perfil impróprio para que possamos rever.

## YouTube

Se encontrar um vídeo no YouTube que considere que viola as nossas Regras da Comunidade, pode denunciá-lo como impróprio e o mesmo será avaliado pela nossa equipa. Lembre-se de que, ao utilizar o Modo de segurança do YouTube, pode filtrar conteúdo que, embora cumpra as nossas Regras da Comunidade, prefere não ver.

## Blogger

Quando leem blogs alojados no Blogger, os utilizadores podem denunciar material que considerem que viola as políticas do Blogger.

Saiba como utilizar estas ferramentas em [www.google.pt/goodtoknow/familysafety/abuse](http://www.google.pt/goodtoknow/familysafety/abuse)



### 3. Saber como a Google o ajuda a proteger-se

A Internet é fantástica. Mas, tal como no mundo offline, nem todas as pessoas online têm boas intenções. A Google leva a sua privacidade e segurança muito a sério. Investimos milhões de dólares por ano e empregamos especialistas de renome mundial na segurança de dados, para manter as suas informações seguras. Estes concentram-se em mantê-lo a si e às suas informações em segurança e a ficar um passo à frente dos cibercriminosos.

A Google trabalha arduamente para ajudá-lo(a) a proteger-se do roubo de identidade, fraude pessoal e esquemas fraudulentos online, para ajudar a proteger o seu computador e tornar a Internet num local mais seguro. Damos-lhe as ferramentas e o conhecimento de que precisa para se manter a si e à sua família em segurança online. E estamos constantemente a investir e a melhorar para agir em seu nome.

## Ajudar a combater o roubo de identidade

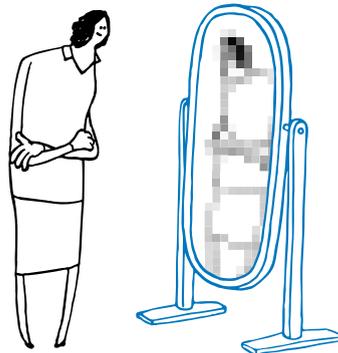
A Google utiliza várias tecnologias para ajudar a protegê-lo contra o roubo de identidade online e certificar-se de que a sua Conta Google permanece segura e protegida.

### Confirmação em 2 passos

Para a sua Conta Google ter níveis de proteção ainda mais fortes, oferecemos a confirmação em dois passos aos nossos utilizadores. Esta ferramenta adiciona um nível de segurança adicional, exigindo não apenas uma palavra-passe, mas também um código de confirmação, para iniciar sessão numa Conta Google. Mesmo que a sua palavra-passe seja decifrada, adivinhada ou roubada, um utilizador mal intencionado não pode iniciar sessão na sua conta sem introduzir o código de confirmação que iremos enviar para o seu telemóvel.

### Encriptação

A Google toma várias medidas para manter as suas informações pessoais a salvo de utilizadores mal intencionados e bisbilhoteiros. Por predefinição, encriptamos a ligação do Gmail entre o seu computador e a Google, pois isso ajuda a proteger a sua atividade Google de ser vista por outros. Também tornamos esta proteção, conhecida como encriptação SSL em toda a sessão, na predefinição quando tem sessão iniciada no Google Drive e em muitos outros serviços.



# Trabalhar para ajudar a manter o seu computador e dispositivo limpos

Pode ajudar a proteger o seu computador contra programas maliciosos, mas a Google também trabalha arduamente para o(a) proteger, graças a centenas de especialistas em segurança que trabalham permanentemente para ajudar a garantir que os seus dados e dispositivos estão seguros.

## **Ajudá-lo a evitar programas maliciosos**

Tal como a Google pesquisa na Web à procura de sites com as melhores respostas para as suas perguntas, também procuramos sites que parecem ser prejudiciais para os utilizadores ou que têm programas maliciosos. Todos os dias, identificamos e denunciámos mais de 10 000 desses sites inseguros e mostramos avisos num número de resultados da Pesquisa Google que pode chegar aos 14 milhões e em 300 000 transferências, dizendo aos nossos utilizadores que poderá haver algo suspeito a ocorrer num determinado Website ou link.

## **Ajudá-lo a manter o seu dispositivo móvel seguro**

Os smartphones com software Android da Google têm proteções semelhantes instaladas para reduzir o risco de danos. O Android também requer que todas as aplicações na Google Play Store listem que tipo de informação a aplicação tem de recolher ou aceder no seu dispositivo, para que possa decidir se confia ou não na aplicação. Também analisamos automaticamente o Google Play para bloquear e remover aplicações prejudiciais e, para alguns telemóveis Android, o nosso Serviço de Verificação de Aplicações da Google irá verificar se existem aplicações potencialmente prejudiciais, independentemente do local a partir do qual as está a instalar.



# Tornar a Internet mais segura para todos

Proteger os utilizadores é uma responsabilidade partilhada. Estamos todos melhor quando todos utilizam as melhores tecnologias e técnicas de segurança.

## Partilhar conhecimentos e ferramentas

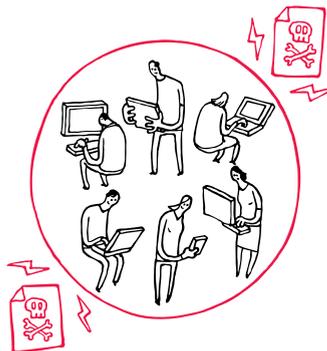
Porque a sua segurança é importante para nós independentemente dos serviços ou produtos que está a utilizar, partilhamos a informação acerca de Websites e links maliciosos que encontramos com outras empresas, para que possam ajudar a proteger também os seus utilizadores. Ao trabalhar em conjunto e ajudando-nos uns aos outros, a Web é toda muito mais segura.

## Comunicar com utilizadores e proprietários de Websites

À medida que trabalhamos para proteger os nossos utilizadores e as suas informações, por vezes descobrimos e investigamos padrões de atividade invulgares. Identificamos e denunciemos diariamente mais de 10 000 desses sites inseguros. Também enviamos mensagens todos os dias para milhares de proprietários de sites que achamos que podem ter sido comprometidos por um ataque para que possam limpar os seus sites.

## Fazer parceria com organizações de segurança

A Google faz parte de várias organizações que trabalham para ajudar empresas a melhorar a segurança dos seus utilizadores. Por exemplo, ajudámos a fundar e fizemos parceria com a StopBadware.org para tornar a Web mais segura, interrompendo, reduzindo e limpando Websites com programas maliciosos ou outro software malicioso.







internet  
seguraopt

Para obter mais informações sobre como se manter seguro(a) online, aceda a  
[www.google.pt/goodtoknow](http://www.google.pt/goodtoknow)