cartilha de **segurança** em **redes sociais**

RNP CAIS

sumário

Redes Sociais são uma parte importante do dia a dia de todos na Internet. É uma ferramenta de comunicação que assumiu o lugar do e-mail como principal meio de comunicação entre pessoas, influenciando suas vidas de várias formas. Nesta cartilha, o CAIS oferece dicas para o uso seguro das redes.

recomendações **gerais**

Entenda que redes sociais não combinam muito com privacidade. De maneira geral, as configurações padrão das redes sociais oferecem proteção de privacidade insatisfatória, mas você pode fazer alterações nas configurações de cada perfil.

Ao terminar sua sessão de uso em qualquer site de rede social, lembre-se sempre de clicar em *Sair/Logout*. Isso é muito importante para evitar que outras pessoas usem sua conta, seja em sua própria máquina ou em máquinas de terceiros. Redes sociais armazenam dados tão íntimos quanto uma conta de *e-mail*. Isso é particularmente importante para o Google+, já que uma sessão aberta permite acesso a qualquer serviço Google (Gmail, YouTube, entre outros).

Seja muito criterioso na hora de aceitar convites, especialmente em redes sociais que não fornecem muitos dados sobre o usuário, como o Twitter. Antes de aceitar um novo seguidor, observe se você reconhece a pessoa pela foto. Perfis sem atualizações e que seguem centenas de usuários podem ser fraudulentos.

Simplifique a "gerência" de seu perfil, particularmente no Facebook, aceitando pedidos de amizade somente de familiares e amigos próximos. Evite participar

de muitos grupos, pois a criação de diversos grupos com regras distintas adiciona complexidade desnecessária.

Os padrões de uso de Internet mudaram muito desde o advento das primeiras mídias sociais, há mais de dez anos. As principais mudanças foram o uso massivo de dispositivos móveis (*smartphones*, *tablets*) e uma navegação mais centrada em redes sociais. É natural que as ameaças digitais se adaptem a essas mudanças comportamentais, por isso espere receber conteúdo malicioso também por meio desses canais.

Use pelo menos 12 caracteres ao criar uma senha nas redes sociais. Para aumentar a força de sua senha, utilize números, letras maiúsculas e minúsculas, alguns caracteres especiais ("_" e "-" são os mais indicados). Os sites normalmente indicam qual é a "força" de sua senha (***Forte***, ***Fraca***, ***Muito Forte***). Procure não repetir a mesma senha em outros serviços. Você pode usar o site ***Random.org*** para gerar senhas: *https://www.random.org/passwords/?num=5&len=12&format=html*

Utilize um software para gerenciar suas senhas. Sugerimos o ***KeePass*** que, além de armazenar suas senhas, ainda ajuda a gerar novas, caso necessário. O programa tem versão disponível para Microsoft Windows, GNU Linux e Apple Mac OS X, Google Android e Apple iOS. Mais informações em *http://keepass.info*

Você pode usar senhas menos complexas (8 caracteres), desde que escolha utilizar "***verificação em duas etapas***", que basicamente consiste em uma senha estática (a que você define) e outra senha temporária enviada por SMS ou *app* de *smartphone*/*tablet* (normalmente ***Google Authenticator***). Sugerimos que use, sempre que possível, a opção SMS. Dessa forma, se você perder seu *smartphone*/*tablet*, ou mesmo se a bateria acabar, o processo de autenticação não será comprometido.

Troque sua senha com frequência, especialmente quando utilizar o serviço de redes sociais em locais públicos como redes Wi-Fi de aeroportos, eventos, *lan houses* ou no computador de outra pessoa.

Impeça que as redes sociais o sigam quando você está visitando outros *sites*. Instale a extensão de navegador ***Disconnect***, disponível em *https://disconnect.me*

Ao criar sua conta, nunca escolha a opção de convite de amigos pela importação de seus contatos *Gmail* / *Yahoo* / *Outlook.com*.

Formulários de Internet não são formulários de IRPF.

× Nem todos os campos são obrigatórios.

× Preencha somente o mínimo. O mesmo serve para cadastros em lojas "físicas".

× Evite: Telefone, Endereço, indicar quem é familiar/esposo, onde estudou/estuda (***LinkedIn é mais apropriado***), onde trabalhou / trabalha (***LinkedIn***).

× Lembre-se sempre de fornecer nenhuma informação para quem não é de sua rede, e pouca informação sobre você. O mais importante das redes sociais está na interação, não em seus dados pessoais.

Evite enviar fotos particulares ou íntimas. É difícil controlar o destino dessas fotos, mesmo que seu grupo de amigos seja bem reduzido. Desabilite também o envio de posição GPS em seu *smartphone*.

Não faça *login* em *sites* de terceiros usan-

do sua conta do Facebook/Twitter/Google Plus/LinkedIn (Conectar com Facebook etc.). Ao fazer isso, você normalmente permite o acesso a vários dados privados de seu perfil. Prefira criar uma conta no próprio *website*.

Por final, não autorize que uma rede social atualize outra (*Tweets* a partir do Linkedin por exemplo). Esse recurso é um dos principais facilitadores de "invasão" de perfil. Assim você minimiza o risco de comprometimento completo de sua reputação em redes sociais no caso de um acesso não autorizado.

Nessa seção oferecemos algumas dicas sobre como criar e manter um perfil nas principais redes sociais usadas no Brasil de maneira mais segura e privativa. É bom lembrar que os recursos e configuração de perfil de redes sociais são muito dinâmicos e podem mudar a cada semana. Por essa razão, é possível que nomes e telas não sejam exatamente os mesmos que você verá nessa cartilha, mas as recomendações gerais podem ser utilizadas.

recomendações **específicas**

facebook

Facebook é possivelmente a rede social com configuração mais complexa entre as quais abordaremos. As configurações que sugerimos concentram-se nas seguintes seções da configuração do perfil (ícone de engrenagem): ***Segurança***, ***Privacidade***, ***Bloqueio***, ***Aplicativos***.

» seção "segurança"

(https://www.facebook.com/settings?tab=security)

- **Notificações de *login*:** Ative essa opção, que basicamente informa caso alguém tente acessar sua conta.

- **Aprovações de *login*:** Esse é um recurso pouco conhecido do Facebook, e consiste basicamente em autenticação em duas etapas.

- **Gerador de códigos:** Cria um código de segurança a cada 30 segundos, mesmo quando você não está conectado à Internet. Você poderá usar esse código, além da sua senha, para fazer *login* no Facebook. Você também poderá usar o Gerador de códigos se precisar redefinir sua senha.

- **Senha de aplicativos:** Esse é outro excelente recurso de segurança, útil para quem costuma autorizar aplicações de

terceiros (Skype, Kindle etc.) a usar sua conta do Facebook. Através dessa opção você pode definir uma senha para cada um desses aplicativos, que pode ser revogada a qualquer momento.

Contatos de confiança: Selecione de três a cinco amigos para quem você possa telefonar para pedir ajuda caso ocorra algum problema com a sua conta. Os amigos escolhidos serão notificados.

Navegadores confiáveis: Visite essa seção com frequência. Essa opção permite que você desautorize dispositivos que você autorizou anteriormente (um computador alheio, um celular que foi roubado ou perdido, por exemplo).

Onde você está conectado: Visite essa seção com frequência. Essa opção permite que você feche sessões que em que esqueceu de finalizar a sessão (navegador fechado sem *logout* e *cookies* apagados, uso de seu perfil em computador alheio). Remova sessões mais antigas ou diferentes de "este dispositivo". É possível que você precise fazer *login* novamente.

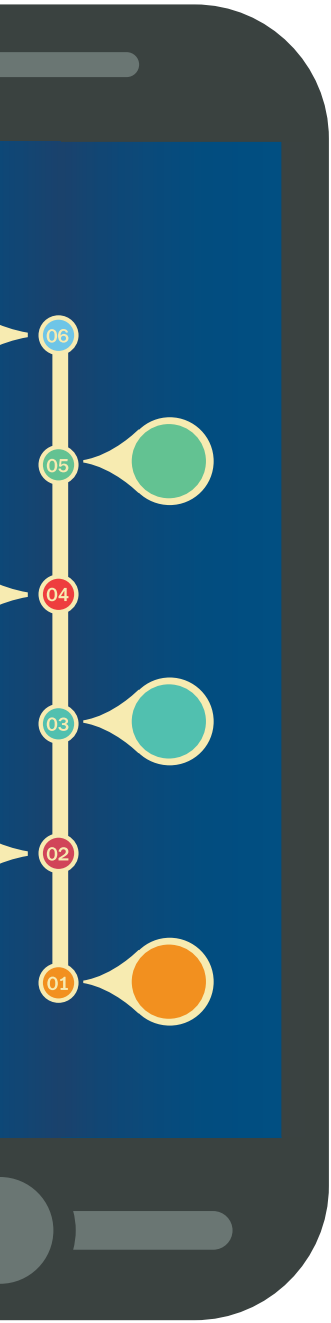
» seção “privacidade”

(https://www.facebook.com/settings?tab=privacy)

- **Opção “Quem pode ver minhas coisas?”**
  - **Quem pode ver suas publicações futuras?** Escolha a opção “*Amigos*”.
  - **Analisar todas as suas publicações e os itens em que você foi marcada.** Escolha a opção “*Usar o registro de atividades*”.
  - **Limitar o público para as publicações que você compartilhou com Amigos de Amigos ou Público?** Escolha a opção “*Limitar publicações anteriores*”.

- **Opção “Quem pode entrar em contato comigo?”**
  - **Quem pode lhe enviar solicitações de amizade?** Escolha da opção a seu critério.
  - **De quem desejo filtrar as mensagens na minha caixa de entrada?** Escolha a opção “*Filtragem restrita*”.

- **Opção “Quem pode me procurar?”**
  - **Quem pode procurar por você usando o endereço de *e-mail* fornecido?** Escolha a opção “*Amigos*”.
  - **Quem pode procurar por você usando o número de telefone fornecido?** Escolha a opção “*Amigos*”.
  - **Você deseja que outros mecanismos de busca**



exibam um *link* da sua linha do tempo? Escolha a opção "***Não***".

» seção "linha do tempo e configurações de marcações"

(https://www.facebook.com/settings?tab=timeline)

▶ Opção "Quem pode adicionar conteúdo à minha linha do tempo?"

× **Quem pode publicar em sua linha do tempo?** Escolha a opção "***Somente eu***".

× **Analisar publicações nas quais amigos marcam você antes de serem exibidas na sua linha do tempo?** Essa é uma configuração muito importante. Escolha a opção "***Ativada***". Dessa forma, pessoas não podem marcar você em fotos e outros conteúdos sem sua autorização.

▶ Opção "Quem pode ver publicações na minha linha do tempo?"

× **Quem pode ver publicações nas quais você foi marcado em sua linha do tempo?** Selecione a opção "***Somente eu***".

× **Quem pode ver o que outras pessoas publicam em sua linha do tempo?** Selecione a opção "***Amigos***".

Opção "Como eu faço para gerenciar marcações que as pessoas adicionam e sugestões de marcações?"

- **Analisar marcações que as pessoas adicionam às suas publicações antes de serem exibidas no Facebook?** Essa é outra opção de privacidade importantíssima. Escolha a opção "***Ativada***" para aprovar cada vez em que você for mencionado ou marcado.
- **Quando você for marcado em uma publicação, quem você deseja adicionar ao público caso ainda não esteja adicionado?** Selecione a opção "***Somente eu***".
- **Quem vê as sugestões de marcações quando fotos parecidas com você são carregadas?** Outra opção importante de privacidade. Selecione a opção "***Ninguém***" para evitar a sugestões de marcação de fotos que incluam você ou alguém parecido com você.

» seção “bloqueio”

(https://www.facebook.com/settings?tab=blocking)

Lista restrita: Essa é uma configuração complementar, caso deseje que alguns amigos recebam apenas o conteúdo marcado como ***Público***.

Bloquear usuários: Caso você deseje omitir qualquer atividade de uma pessoa e/ou não quer que essa pessoa veja qualquer atividade sua, essa é a solução mais radical. Trata-se de uma opção que pode lhe causar situações constrangedoras, por isso utilize-a com cuidado.

Bloquear convites de aplicativos: Caso você não deseje receber convites de aplicativos de determinada pessoa.

Bloquear convites de eventos: Você pode bloquear todos os convites de eventos futuros de determinada pessoa.

Bloquear aplicativos: Ao bloquear aplicativos, você está bloqueando o aplicativo independente da pessoa que envie o convite.

» seção “seguidores”

(https://www.facebook.com/settings?tab=followers)

Quem pode me seguir. Permite que pessoas sigam seu perfil de uma maneira semelhante ao Twitter. Se você deseja mais privacidade não marque essa opção.

» seção “aplicativos”

(https://www.facebook.com/settings?tab=applications)

Há uma seção equivalente a essa em todas as outras redes sociais cobertas por esta cartilha. Entretanto, no Facebook, Linkedin e Google+ a boa gerência dessa seção é mais crítica porque essas redes sociais manipulam muito mais dados pessoais do que o Twitter, por exemplo.

De maneira geral, nossa dica é sempre a mesma para essa seção: revogar todos os acessos periodicamente (uma vez ao mês, por exemplo)

para assegurar que nenhuma aplicação indesejada tenha acesso completo a seu perfil.

- **Aplicativos que você usa:** Essa é outra opção muito importante. Remova todos os aplicativos que você não utiliza mais.

- **Aplicativos usados por outras pessoas:** Permita acesso ao mínimo de informações, como ***Atualizações de status*** e ***Meus links***.

- **Personalização instantânea:** Não marque ***Ativar*** se você deseja fornecer menos dados a sites terceiros.

- **Versões antigas do Facebook para dispositivos móveis:** Escolha a opção "***Somente eu***".

» seção "recursos extras de segurança"

(https://www.facebook.com/help/)

Esta seção é de difícil localização na rede social. No entanto, ela apresenta ***Perguntas e Respostas*** muito úteis para o uso seguro do Facebook, principalmente se você teve sua conta invadida.

Para acessá-la, basta entrar em "***Ajuda***", "***Visite a Central de Ajuda***" e seguir para a aba "***Segurança***".

twitter

Twitter é uma rede social bem menos complexa que o Facebook, mas ainda assim requer cuidados na criação e configuração do perfil. Clique na opção "Configurações" (ícone de engrenagem).

» seção "segurança e privacidade"

(https://twitter.com/settings/security)

Opção "Segurança"

- **Verificação de *login*:** Opção em que é possível verificar que você mesmo fez o *login* na conta, que seria a autenticação de dois fatores.
- **Redefinição de Senha:** Marque a opção "***Pedir informações pessoais para redefinir minha senha***". Ao fazer isso você aumenta a quantidade de dados pessoais necessários ao solicitar a alteração de senha.

Opção "Privacidade"

- **Marcação em fotos:** Selecione a opção mais segura: "***Não permitir que ninguém que eu sigo me marque em fotos***".
- **Privacidade dos *Tweets*:** Desmarque a opção "***Proteger meus Tweets***". Se você deseja controlar melhor quem segue seu perfil, essa é uma boa opção. Entretanto, é bom lembrar que essa opção não impede que alguém cite seu *tweet*, então alguns conteúdos podem vazar assim mesmo.
- **Localização do *Tweet*:** Desmarque a opção "***Adicionar uma localização aos meus Tweets***", caso esteja marcada. Depois, clique no botão "***Apagar todas as informações de localização***". Dessa forma, suas atualizações não serão

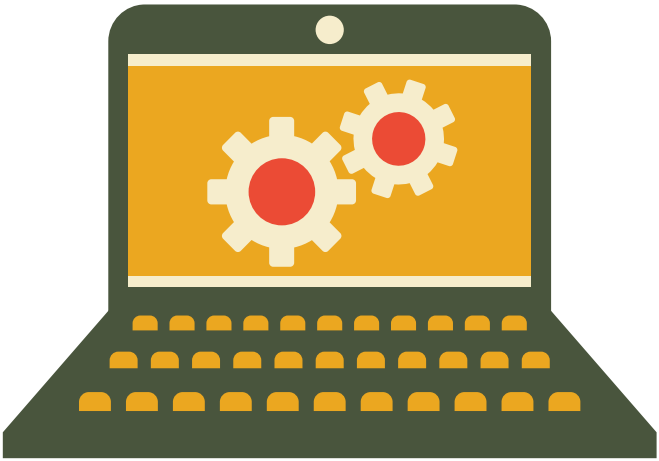
associadas à sua posição geográfica, fornecida por GPS, por exemplo.

× **Descoberta:** Desmarque a opção **"*Permitir que outros me encontrem pelo meu endereço de e-mail*"**. Assim você será encontrado somente se fornecer seu nome de usuário.

» seção perfil

(https://twitter.com/settings/profile)

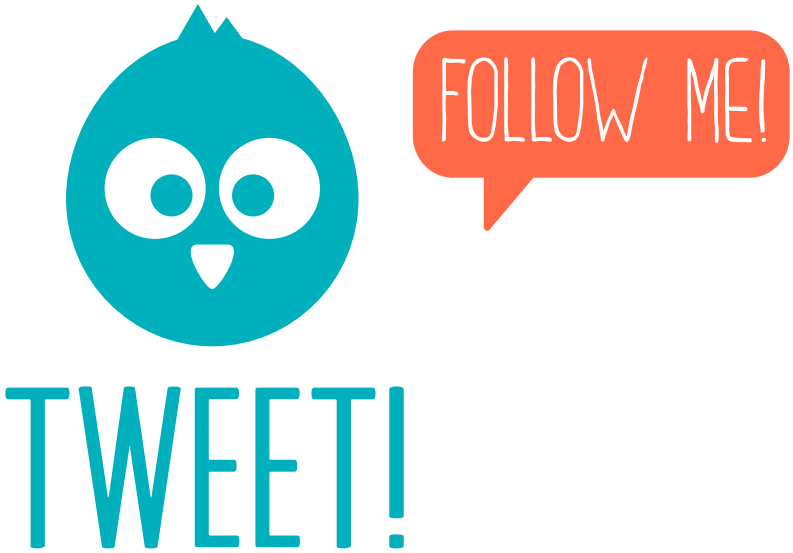
A recomendação geral para essa seção é não fornecer dados em excesso. Em **"*Nome*"**, você não precisa necessariamente fornecer seu nome completo. Em **"*Localização*"**, basta informar Brasil e, em **"*Bio*"**, basta fornecer uma breve descrição.



» seção aplicativos

(https://twitter.com/settings/applications)

Essa é talvez uma das seções mais importantes. É nela que você gerencia quais aplicações têm acesso ao seu perfil. Quando você permite que um aplicativo de *smartphone*, por exemplo, tenha acesso a sua conta no Twitter, o que acontece é o seguinte:



- A aplicação abre *twitter.com* e inicia um processo de autenticação com sua senha principal. Se você já estiver com Twitter aberto, esse passo não acontece. Essa é outra razão da importância do processo de *logout*/sair em redes sociais.

- Uma vez completada a autenticação, você deve confirmar que permite que esse aplicativo ou *website* terceiro tenha acesso a seu perfil Twitter.

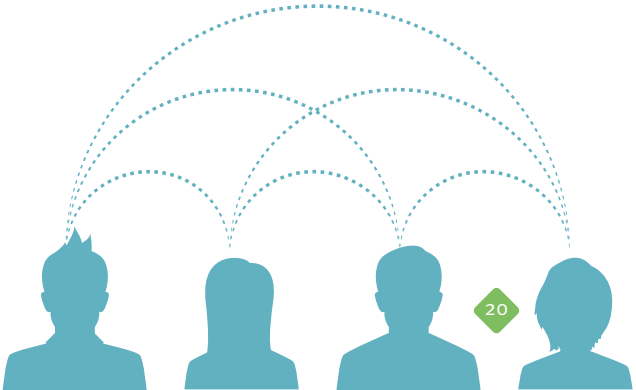
- O aplicativo não armazena sua senha principal, mas sim uma "senha" específica (*token*) para aquele aplicativo. Quando você revoga o acesso de um determinado aplicativo esse *token* é apagado.

Recomendamos que você revogue o acesso a todas as aplicações ao menos uma vez por mês. Dessa forma, você bloqueia o acesso às aplicações que não utiliza mais e dificulta o roubo de sua conta, especialmente quando utiliza o Twitter em *hotspots* Wi-Fi.

linkedin

Linkedin é uma rede social criada com intuito profissional. Seu propósito é bem diferente do Facebook e Google+, que têm todos os seus recursos voltados ao uso pessoal. Os principais propósitos do Linkedin são representar sua rede profissional na forma de uma rede social e, de certa forma, substituir os cartões de visita.

Recomendamos que você separe radicalmente sua vida profissional de sua vida pessoal nas redes sociais. Isso significa não inserir dados sobre trabalho no Facebook (onde trabalha, fazer amizade com simples colegas de trabalho), por exemplo. Dessa maneira, é mais fácil evitar incidentes que comprometam sua reputação profissional, como fotos comprometedoras, opiniões polêmicas ou mesmo atualizar a rede social durante o expediente de trabalho.



Assim como acontece no Facebook, o Linkedin também tem as configurações de perfil um pouco complexas. A seguir, você encontrará dicas para reforçar a segurança e privacidade no uso dessa rede social.

As opções interessantes para segurança e privacidade estão em "***Configurações e Privacidade***" (*https://www.linkedin.com/settings*).

» seção perfil

Ativar/Desativar divulgação de atividades e status: Clique nessa opção e marque a caixa de seleção. Dessa forma, você pode usar a rede social sem se preocupar com colegas de trabalho ou superiores monitorando suas atividades, que muitas vezes podem indicar uma busca por mudança de emprego.

Selecionar quem pode ver o seu *feed* de atividades: Essa é uma opção muito importante. Clique nessa opção e selecione "***Suas conexões***". Assim, quem não estiver em sua rede não verá o seu *feed* de atividades (semelhante à *timeline* ou linha do tempo no Facebook).

Selecionar o que as pessoas verão após sua visita ao perfil das mesmas: Essa opção também é muito importante. Recomendamos que você escolha a opção "***Você permanecerá como um usuário anônimo***" ou "***Características anônimas do meu perfil, como setor e cargo***", nessa ordem. Infelizmente, a primeira está disponível apenas em contas do tipo ***Premium*** (pagas).

Selecionar quem pode ver suas conexões: Essa opção determina quem pode ver sua lista completa de conexões. Por razões de privacidade e estratégia de carreira, recomendamos que você escolha a opção "***Somente você***".

Editar seu perfil público: Recomendamos que você não tenha um perfil público. Dessa forma, não é possível encontrar informações detalhadas sobre seu perfil em mecanismos de busca. Para ter acesso mínimo a seu perfil será necessário ser usuário do Linkedin.

» seção grupos, empresas e aplicativos

Visualizar seus aplicativos: Como afirmamos anteriormente, é nessa seção que você gerencia o acesso de aplicativos de terceiros ao seu perfil. Nossa recomendação é a mesma que para as outras redes sociais: revogar periodicamente os acessos.

Ativar/Desativar compartilhamento de dados com aplicativos parceiros: Desmarque essa opção.

Gerenciar configurações de *plugins* do LinkedIn em *sites* de terceiros: Desmarque essa opção. De qualquer forma, se você instalar a extensão de navegador ***Disconnect*** (consulte a seção ***Recomendações Gerais***) esse problema já estará de certa forma tratado.

» seção conta

Alterar foto de perfil e visibilidade: É importante ter sua foto no perfil criado no Linkedin. Entretanto, se você deseja que apenas sua rede visualize sua

foto, marque a opção "*Minha rede*" em "*Além dos usuários para quem envio mensagens, minha foto de perfil estará visível para...*".

Gerenciar configurações de segurança: Essa é outra seção importantíssima. Nela você habilita SSL (conexão cifrada que evita a captura de seus dados) e habilita a autenticação em duas fases por meio de SMS. O Linkedin tornou-se um elemento crítico na carreira de muitos profissionais. É fundamental que essas duas opções sejam habilitadas para mitigar o risco de roubo de conta.

google+ (google plus)

Google+ é uma rede social lançada em 2011 pelo Google. Embora seja uma rede grande (já ultrapassou o Twitter em 2013), não é muito conhecida, embora integre de maneira sutil todos os serviços do Google. No Brasil, muitas pessoas podem estar nessa rede sem saber apenas por usar serviços Google como Gmail, YouTube, Orkut ou mesmo *smartphone* Android.

A seguir, oferecemos algumas dicas de segurança e privacidade para esta rede social.

como saber se estou no google+?

A maneira mais fácil de saber se você possui um perfil no Google+ é realizar *login* em algum serviço Google (Gmail, por exemplo) e depois abrir a seguinte página:

https://plus.google.com

Se esta página for um convite a criar um perfil, você não está Google+. Caso você tenha um perfil e deseje sair do Google+, visite a seguinte página e escolha a opção "***Excluir o conteúdo do Google+***":

https://plus.google.com/u/o/downgrade

» dicas de segurança e privacidade

Assim como as demais redes sociais, as contas Google+ por padrão não são configuradas com um nível aceitável de privacidade.

Em primeiro lugar, recomendamos que você ative a autenticação em duas etapas. Essa simples ação dificulta muito a "invasão" de sua conta por um terceiro ou até mesmo por uma pessoa conhecida com más intenções (ex-namorado(a), competidores, inimigos). Para isso, visite a seguinte página e associe sua conta Google a seu celular:
https://accounts.google.com/b/o/SmsAuthLanding

As primeiras recomendações se aplicam para a conta Google+. Clique em sua foto no canto direito superior da janela e depois em "***Conta***". Na tela seguinte, clique em "***Editar configurações***". Se preferir, simplesmente clique no *link* a seguir:
https://plus.google.com/settings

O Google+ é tão complexo quanto o Facebook, por isso recomendamos que você adote a mesma estratégia: tenha poucos "***círculos***" de amigos. Se possível, tenha somente um.

Quem pode interagir com você e com suas postagens: Escolha "***Seus círculos***" para todas as opções. Dessa forma, você limita o universo de pessoas que podem entrar em contato com você a apenas seus contatos, que no Google+ são organizados na forma de "***Círculos***".

Quem pode participar de um Hangout com você: A aplicação Google Talk está sendo substituída gradualmente pelo Google Hangouts. Clique em "***Personalizar***" e determine quem pode participar de um *hangout* com você. Recomendamos que você escolha "***Somente convidados***" para todas as opções.

Aplicativos e atividades: Essa opção é muito semelhante ao gerenciamento de aplicações de terceiros de *sites* como o Linkedin, Twitter e Facebook. Recomendamos que você remova todos os aplicativos periodicamente. Clique no botão "***Gerenciar aplicativos***" para fazer isso.

Seus círculos: Clique no botão "***Personalizar***" para escolher o alcance de suas atualizações. Recomendamos que selecione somente o círculo "***Amigos***".

Fotos e vídeos: Estas configurações são muito importantes. Não marque nenhuma das opções, principalmente a opção sobre mostrar informações de localização geográfica em fotos e vídeos. Isto possibilita que alguém mal intencionado tenha acesso a sua localização e saiba dos locais que você frequenta.

» perfil

× **Mostrar minhas postagens em comunidades do Google+ na guia "Postagens" do meu perfil do Google+:** Desmarque essa opção.

× **Permitir o envio de mensagem a você diretamente do seu perfil:** Assegure-se que esta opção esteja desmarcada ou marcada e com a opção "***Somente você***" ou "***Seus círculos***" selecionada.

× **Ajudar outras pessoas a encontrar meu perfil em resultados de pesquisa:** Desmarque essa opção para evitar que seu perfil seja encontrado em buscas no Google.

Configurações de local: Assegure-se que a opção "***Ativar compartilhamento de local***" esteja desmarcada. Caso deseje ativar essa opção, recomendamos que selecione a opção "***Somente você***" ou "***Seus círculos***".

Uma configuração adicional é remover o máximo de dados possível no seu perfil. Para isso, abra a página *https://plus.google.com*, clique em **"*Início*"** (à esquerda, ícone de uma casa), depois selecione **"*Perfil*"** e, finalmente, a opção **"*Sobre*"** (topo da página).

Em ***Pessoas***, clique em **"*Editar*"** e desmarque as opções **"*Exibir as pessoas em seus círculos*"**. Desmarque também a opção **"*Mostrar as pessoas que adicionaram você aos seus círculos*"**.

É interessante também editar a opção Informações básicas. Recomendamos que você clique em **"*Editar*"**. Na seção **"*Sexo*"**, selecione a opção **"*Seus círculos*"**. Na seção **"*Aniversário*"**, escolha a opção **"*Seus círculos*"**. No mais, recomendamos que você forneça o mínimo de dados possível. Evite informar quem é seu namorado ou namorada e familiares.

Para mais informações sobre como deixar seu perfil no Google+ mais seguro, acesse logo abaixo de sua foto de perfil o *link* **"*Privacidade*"**. Essa página contém dicas de segurança, ***Termos de Serviço*** e a ***Política de Privacidade***. Você também pode acessá-la diretamente através do *link*: *http://www.google.com.br/intl/pt-BR/policies*

Confira as iniciativas e projetos de segurança da informação promovidos pela RNP em:
http://www.rnp.br/servicos/seguranca