



Segurança em redes sociais: recomendações gerais

Centro de Atendimento a Incidentes
de Segurança (CAIS/RNP)



RECOMENDAÇÕES GERAIS

- Seja criterioso na hora de aceitar convites, especialmente em redes sociais que não fornecem muitos dados sobre o usuário, como o Twitter. Observe se você reconhece a pessoa pela foto e o número de amigos ou seguidores. Amigos demais podem indicar perfis fraudulentos.
- Use pelo menos 8 caracteres na sua senha. Utilize números, letras maiúsculas e minúsculas, alguns caracteres especiais (“_” e “-” são os mais indicados). Os sites normalmente indicam se a senha que você escolheu é “Forte” ou não. Escolha senhas que indiquem “Strong” (Forte) ou “Very Strong” (Muito forte). Não use a mesma senha de outros serviços!
- Use um software para gerenciar suas senhas. Sugerimos KeePass, que além de armazenar suas senhas o ajuda a escolher boas combinações. O programa é disponível para Microsoft Windows, GNU Linux e Apple Mac OS X, e pode ser acessado em <http://keepass.info/>
- 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.
- Sempre saia do serviço adequadamente, usando o link “logout”. Se você não fizer isto a próxima pessoa que usar o computador terá acesso à sua conta. O logout também fecha as sessões abertas em outros computadores e celulares que você utilizou. Se você esqueceu-se de efetuar logout em uma rede potencialmente insegura, troque a senha o mais rápido possível. A sessão que você deixou aberta será interrompida e a senha será solicitada.
- É muito comum o uso de encurtadores de endereço, os chamados URL shorteners. Estes serviços encurtam endereços longos de forma que eles sejam curtos o suficiente para serem enviados por e-mail, Twitter, etc. Estes serviços são representados por sites como bit.ly (j.mp), TinyURL e Migre.me, entre outros. Mas atenção: é muito comum a distribuição de vírus usando estes serviços para esconder o endereço final. Alguns serviços possuem ferramentas especiais para que você visualize informações adicionais antes de visitar o link final. Conheça alguns deles: Bit.ly: Inclua “+” ao final ou /info/ para mais informações. Por exemplo, se a URL for <http://bit.ly/S4YAc>, acesse <http://bit.ly/S4YAc+> ou <http://bit.ly/info/S4YAc>.
- TinyURL.com: para mais informações, inclua “preview” no início do endereço. Por exemplo, para a URL <http://tinyurl.com/ygqyjd8> tente <http://preview.tinyurl.com/ygqyjd8>.





ORKUT

Para utilizar o Orkut é necessário possuir uma conta no Google (Google Account). Esta conta é a mesma utilizada por serviços como Gmail, Picasaweb, Blogger (Blogspot), Google Agenda, Google Docs, Google Talk, entre outros. Se possível crie uma nova conta para uso exclusivo para Orkut. Para isto basta sair (logout) de um serviço Google antes de se cadastrar no Orkut para criar uma nova conta Google. Talvez seja necessário fornecer o número de seu celular no processo de verificação de identidade. Digite seu celular no formato +55XX55551234, onde XX é o código de área (DDD). Digite o código que receber no celular por SMS (“torpedo”) na tela de verificação.

Defina uma senha forte, conforme as recomendações desta cartilha.

Ao informar seus primeiros dados pessoais (data de nascimento, primeiro e último nome, gênero, país) se possível informe uma data de nascimento incorreta e anote esta data que você utilizou. Este seu dado pessoal pode ser utilizado para recuperar sua senha ou em fraudes.

figura 1

Ao concluir com sucesso seu cadastro, a seguinte tela será apresentada.

figura 2

Selecione a opção “configurações” do painel esquerdo. Sugerimos que você defina as seguintes opções:

- Na aba “geral”:



figura 3

1. “Filtro de segurança”: marque a opção “não mostrar conteúdo impróprio”

- Na aba “privacidade”:

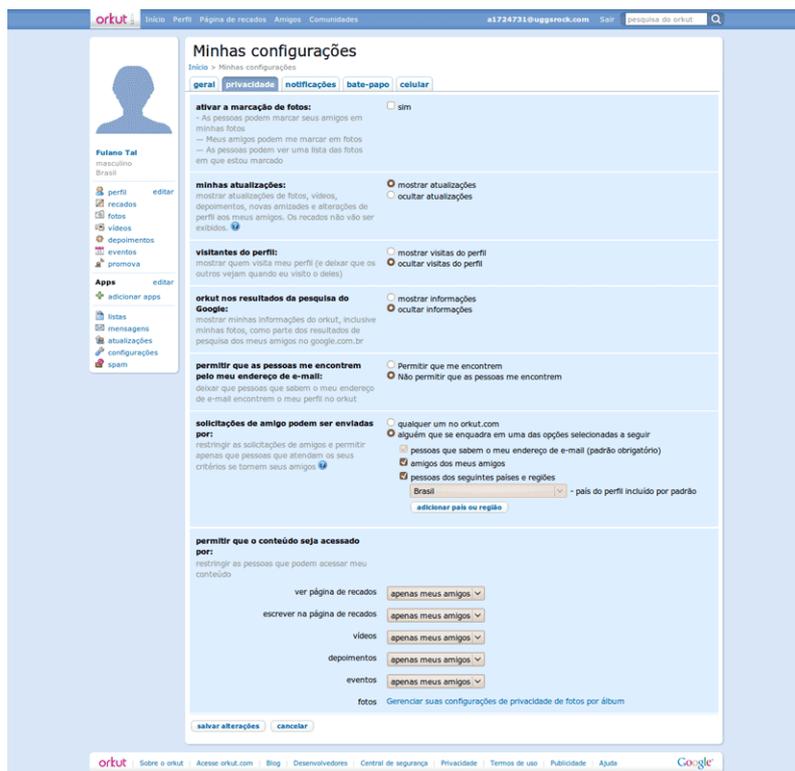


figura 4

1. “Ativar a marcação de fotos”. Marcar “sim” nesta opção permite que outras pessoas identifiquem você em uma foto. Se você for marcado em fotos sem restrições, qualquer pessoa poderá visualizar fotos com você. Se você **não** quer associar fotos de outras pessoas a seu perfil, **não** marque esta opção.

2. "Visitantes do perfil". Marque "Ocultar visitas do perfil". Desta forma você tem privacidade ao visitar o perfil de outras pessoas, e seu perfil não é listado como visitante. Se você deseja monitorar quem visita seu perfil então marque a outra opção ("Mostrar visitas do perfil").
3. "Orkut nos resultados da pesquisa do Google". Marque a opção "Ocultar informações" para que o seu perfil não apareça em pesquisas no site de buscas Google.
4. "Permitir que as pessoas me encontrem pelo meu endereço de e-mail". Marque a opção "Não permitir que as pessoas me encontrem". Desta forma sua privacidade é preservada. Não basta alguém obter seu endereço de e-mail para encontrar seu perfil.
5. "Solicitações de amigo podem ser enviadas por". Marque a opção "Alguém que se enquadra em uma das opções selecionadas a seguir". Quanto mais você puder restringir o universo de pessoas que podem incluí-lo como amigo, melhor. Você evita perfis abusivos que enviam propaganda e até vírus. Selecione a opção "Amigos dos meus amigos". Restringir por região também pode ser interessante, embora o perfil da outra pessoa possa ser configurado com um país incorreto.
6. "Permitir que o conteúdo seja acessado por". Esta escolha é muito importante. O padrão do Orkut é "todos" para todo o seu conteúdo. Ou seja, qualquer perfil pode ter acesso ao seu conteúdo (scraps, vídeos, depoimentos, fotos, etc). Para restringir o acesso ao máximo selecione "Apenas meus amigos" para todos os tipos de conteúdo.

■ Na aba "notificações":

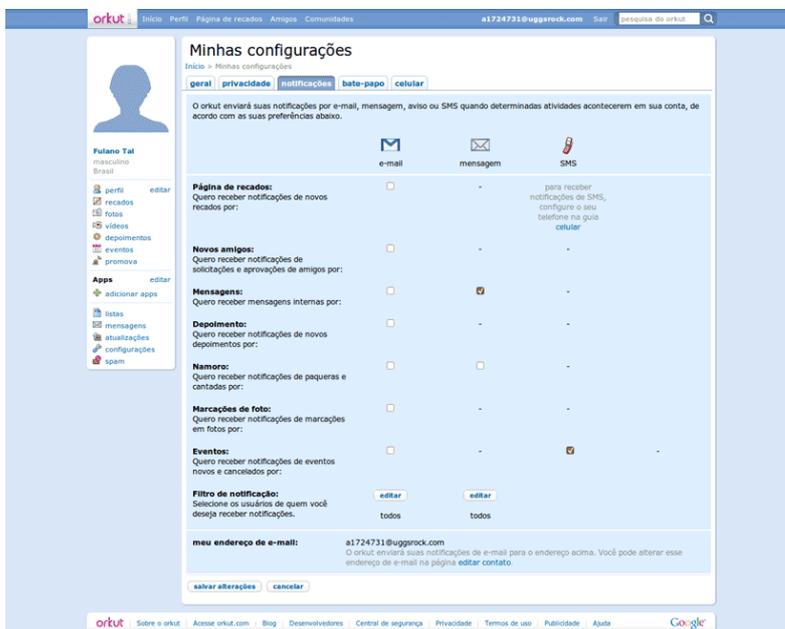


figura 5

1. Se possível desmarque todas as opções da coluna "E-mail". Desta forma você não receberá mensagens com fraudes ou vírus. Esta opção também é interessante porque você saberá de antemão que não deverá receber nenhum e-mail do Orkut. Se receber alguma mensagem muito provavelmente ela será maliciosa.

A seguir selecione a opção “Editar” ao lado de “Perfil”, no painel esquerdo. Sugerimos que você defina as seguintes opções:

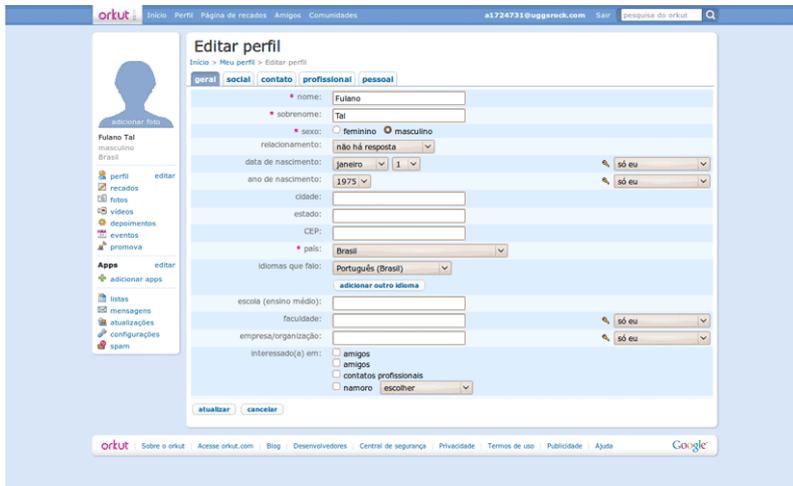


figura 6

1. Para todas as abas (Geral, Social, Contato, Profissional, Pessoal) selecione “só eu” sempre que possível para restringir ao máximo o acesso a dados pessoais. Se esta opção não estiver disponível utilize “Apenas meus amigos”.
2. Não é necessário informar dados sensíveis como CEP, telefone residencial, telefone celular, endereço completo. Apenas Cidade e Estado é aceitável.

Orientações gerais sobre Orkut:

- Apague seus scraps (recados) com frequência.
- Evite se associar a comunidades que informem muito sobre sua rotina. Exemplo: a academia que frequenta, o clube que frequenta, o condomínio em que mora, etc.
- Reúna seus amigos em grupos. Desta forma é possível controlar o acesso a conteúdo (fotos por exemplo) por grupo, restringindo a apenas sua família, por exemplo. Agrupe seus amigos selecionando a opção “Amigos” do painel superior.

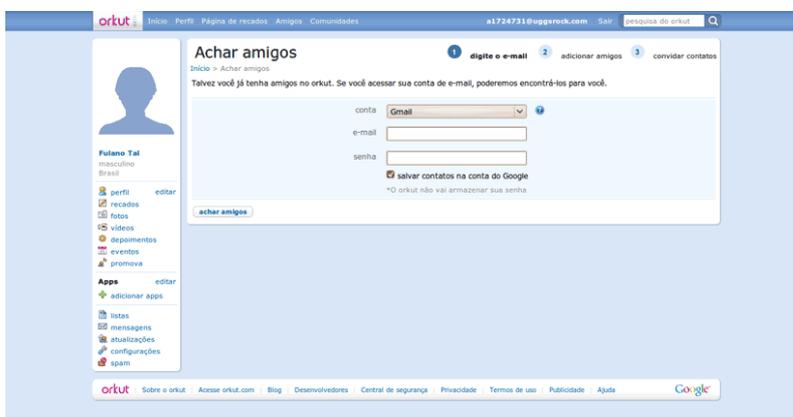


figura 7

Ainda na seção “Amigos”, é possível convidar contatos no Gmail. Selecione “Achar amigos” em “Achar mais amigos”, no painel direito. Você terá que digitar sua senha. Isto é normal, desde que você esteja na página correta.

- Não utilize o Orkut em lan houses, redes abertas de wi-fi e outros lugares de acesso público. É possível capturar suas credenciais de acesso, o que é facilitado pela ausência de conexão segura (**https://** e **cadeado**) que protege os dados entre seu computador e o servidor do Orkut.

- Caso você queira desassociar sua conta Orkut de seus outros serviços Google (Gmail, Picasaweb, etc.), acesse a aba “Geral” da opção “Configurações” (figuras 2 e 3), no painel esquerdo. Para iniciar o processo de exclusão de sua conta Orkut, selecione “Excluir minha conta do Orkut”, no final da página. Exclua apenas a conta no Orkut.



figura 8



figura 9



TWITTER

Recomendações gerais:

Se você usou a opção “Protect my tweets” ao configurar seu perfil no Twitter, cada pessoa que quiser segui-lo terá que pedir permissão. Ao receber estas solicitações verifique se reconhece a foto da pessoa e se você a reconhece pelos tweets. Perfis com milhares de seguidores podem indicar perfis falsos ou de spam.

Recomendações na criação da conta:

- Se possível não utilize seu nome completo.
- Defina uma senha forte, conforme as recomendações desta cartilha.

twitter

Join the Conversation Already on Twitter? Sign in.

Already use Twitter on your phone? Finish signup now.

Full name: Fulano T. ✓ ok

Username: fulanot ✓ ok

Your URL: <http://twitter.com/fulanot>

Password: ●●●●●●●●●● ✓ Very Strong

Email: a2011803@uggsrock.c ✓ ok

I want the inside scoop—please send me email updates!

Type the words above: **waldo 71**

Can't read that?
Get two new words
Hear a set of words
Powered by reCAPTCHA
Help

By clicking on "Create my account" above, you confirm that you accept the [Terms of Service](#).

figura 10

- O Twitter pode procurar contatos no seu Gmail e Yahoo! Mail que usam o Twitter. Isto é normal e será solicitado que você digite seu usuário e senha para realizar esta operação.

twitter

See if your friends are on Twitter

Gmail

Yahoo

AOL

We can check if folks on other services already have a Twitter account. **Choose a service** from the list on the left.

[Skip this step](#)

figura 11



- Esta é a tela inicial no Twitter. Para concluir a configuração mais segura de sua conta selecione a opção “Settings” no canto direito superior da tela. Ainda não há uma versão em Português do Twitter.

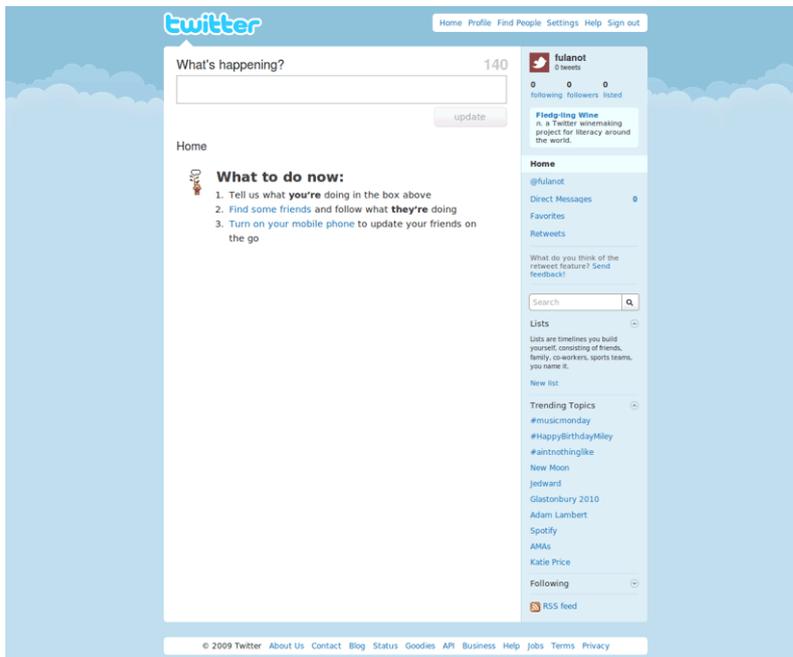


figura 12

- Na tela de configurações (settings):

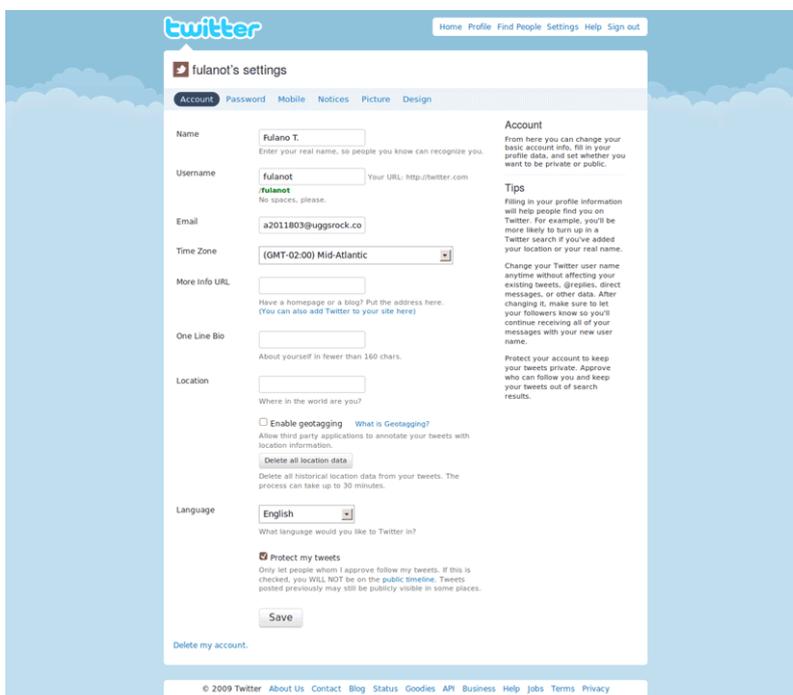


figura 13

1. Name: evite usar seu nome completo. Seus amigos serão capazes de encontrá-lo pelo e-mail.
2. Time Zone: defina o fuso-horário correto, GMT - 03:00 no caso de Brasília, fora do período do horário de verão.

3. More info URL: coloque aqui o link para seu blog ou site, caso queira divulgá-lo. Evite utilizar a página da empresa em que você trabalha. Algumas empresas não permitem isto, além de revelar o seu local de trabalho, um dado pessoal.
4. One Line Bio: descrição curta sobre você. Seja genérico.
5. Location: Local em que você mora. Este campo não é obrigatório, se possível seja genérico e coloque apenas país e/ou estado.

Se você deseja permitir que o Twitter associe seus tweets com a localização geográfica de onde você estiver no momento selecione a opção "Enable geotagging". Se desejar privacidade, desmarque esta opção.

6. Protect my tweets: Se você deseja que as pessoas peçam permissão para ter acesso a seus tweets, marque esta opção. Esta escolha também é boa para evitar que perfis de Spam "sigam" você. Se o perfil no Twitter é destinado a um site e não para seu uso pessoal, esta opção não é recomendada. Você receberá centenas de mensagens de solicitação de acesso ao perfil.

Se você habilitar esta opção será necessário o login no Twitter pelo site para conceder acesso a estes perfis. Aplicativos como TweetDeck, Twhirl e Gravity não executam estas ações.

Se você habilitar esta opções outras aplicações e sites não serão capazes de consultar seus novos tweets em tempo real.

Recomendações no dia a dia:

Vários sites possuem interface com o Twitter, de forma que você efetua login nestes sites com seu usuário e senha Twitter por meio do protocolo OAuth. Isto é normal. Entretanto, seja cuidadoso ao escolher os sites em que você digita suas credenciais de acesso Twitter. Se desconfiar que se cadastrou em um site malicioso, remova o acesso da aplicação a seu perfil e troque imediatamente sua senha. Para controlar o acesso de aplicações a seu perfil visite o seguinte site: <http://twitter.com/account/connections>



Recomendações gerais:

Substitua seu sobrenome pela abreviatura depois da criação da conta.

Recomendações na criação da conta:



figura 14

- Para criar sua conta com Português como idioma padrão, visite a página <http://pt-br.facebook.com/>. Ou selecione “English (US)” no canto inferior esquerdo da página internacional e altere para Português (Brasil).
- Diferente do Twitter, o Facebook oferece a opção de interface em Português. Altere o idioma selecionando “Configurações” e depois “Idiomas”. Altere o idioma de “English (US)” para “Português (Brasil)”.
- Gênero, nome, sobrenome, e data de nascimento são campos obrigatórios.
- Confirme seu endereço de e-mail. Você receberá uma mensagem com um link para confirmação.
- Esta é a tela inicial. Para configurações adicionais e mais segurança, selecione a opção “Configurações”, no canto superior direito da tela.



figura 15

■ Na aba “Configurações”:

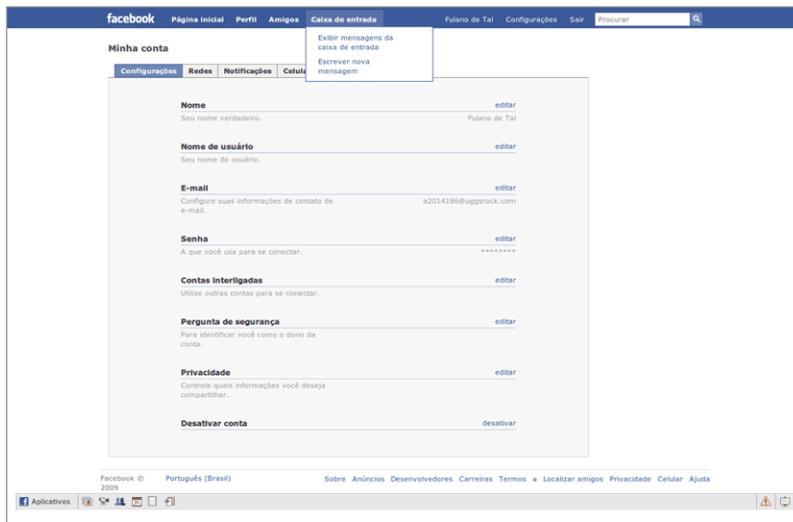


figura 16

1. Pergunta de segurança: escolha uma pergunta da lista apresentada e defina uma resposta. É muito importante que você não responda esta pergunta com a resposta correta, embora isto pareça estranho. É possível investigar sua vida a partir de buscas na Internet e em outras redes sociais e obter as respostas para estas perguntas. Defina uma resposta e anote-a. Este conjunto pergunta/resposta será utilizado no processo de recuperação da senha de sua conta.
2. Privacidade: selecione esta opção para controlar o acesso de outros perfis às suas informações, fotos e outros recursos de seu perfil.

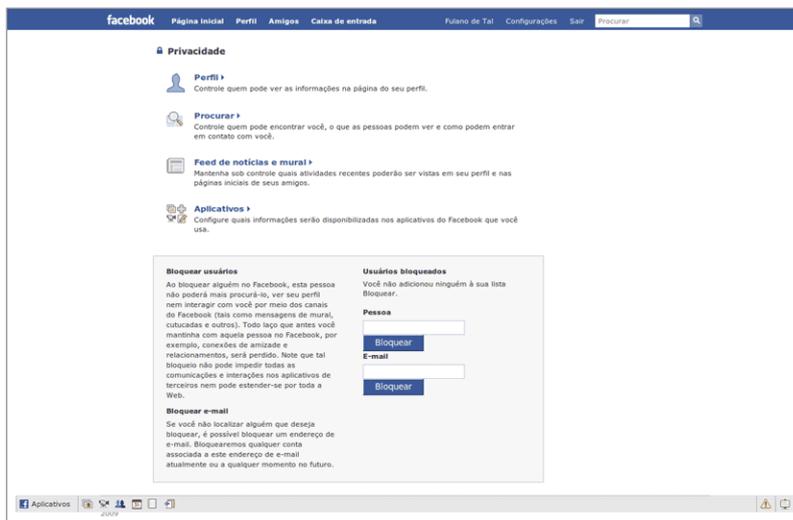


figura 17



Perfil: defina qual será nível de acesso ao seu conteúdo. O nível mais restritivo é “Apenas amigos”.

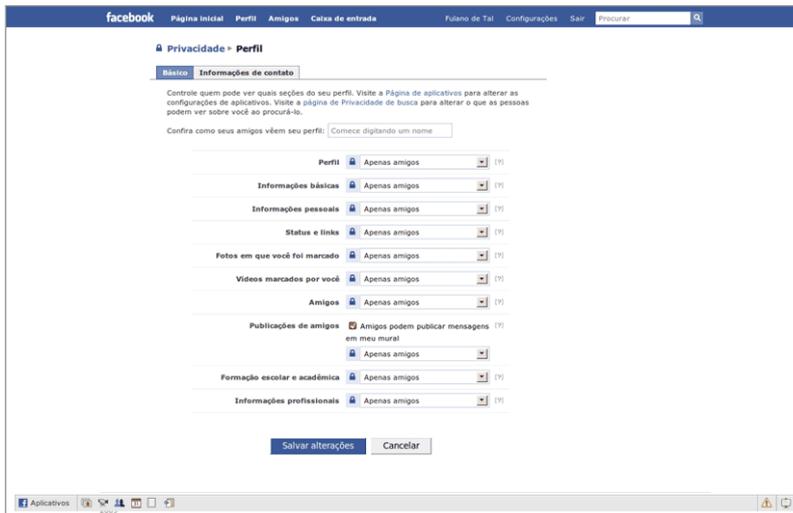


figura 18

Procurar: recomendamos a seguinte configuração para maior privacidade.

- Definir “Apenas amigos” para a opção “Visibilidade de busca”.
- Em “Índice dos resultados de busca” desmarque todas as caixas.
- Em “In addition” desmarque todas as caixas.

Feed de notícias e mural

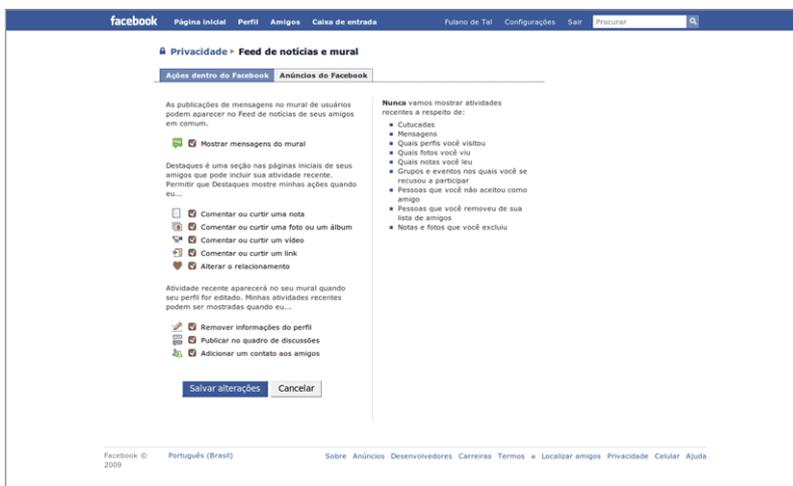


figura 19

- Definir as opções de acordo com o nível de informações pessoais que você deseja divulgar.

Aplicativos: outros sites e aplicações podem ter acesso às informações de seu perfil Facebook. Para maior privacidade recomendamos:

- Aba “Configurações”

Marcar a opção “Não compartilhar nenhuma informação minha através da API do Facebook”

Em “Aplicativos das Conexões do Facebook”, marque a opção “Não permitir que amigos vejam minha associação com outros sites por meio das Conexões do Facebook”.

Em “Sites Beacon” marque a opção “Não permitir que sites Beacon publiquem históricos no meu perfil”.

- Para um controle mais detalhado do acesso de outras aplicações ao seu perfil, visite <https://register.facebook.com/editapps.php>.

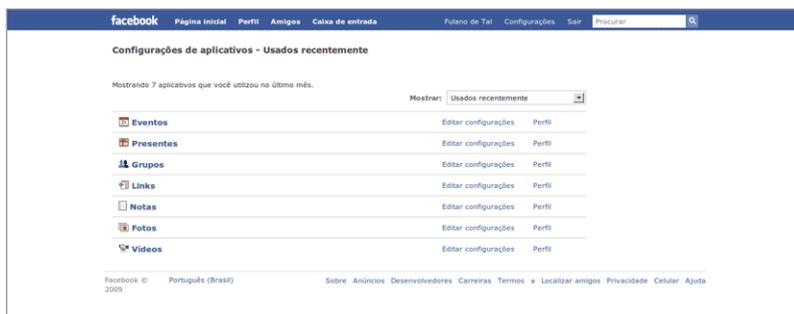


figura 20

■ Na aba “Notificações”

1. Desmarque todas as opções. Desta forma é mais fácil identificar mensagens maliciosas envolvendo o Facebook, já que você não deverá receber nenhuma mensagem a respeito de seu perfil.

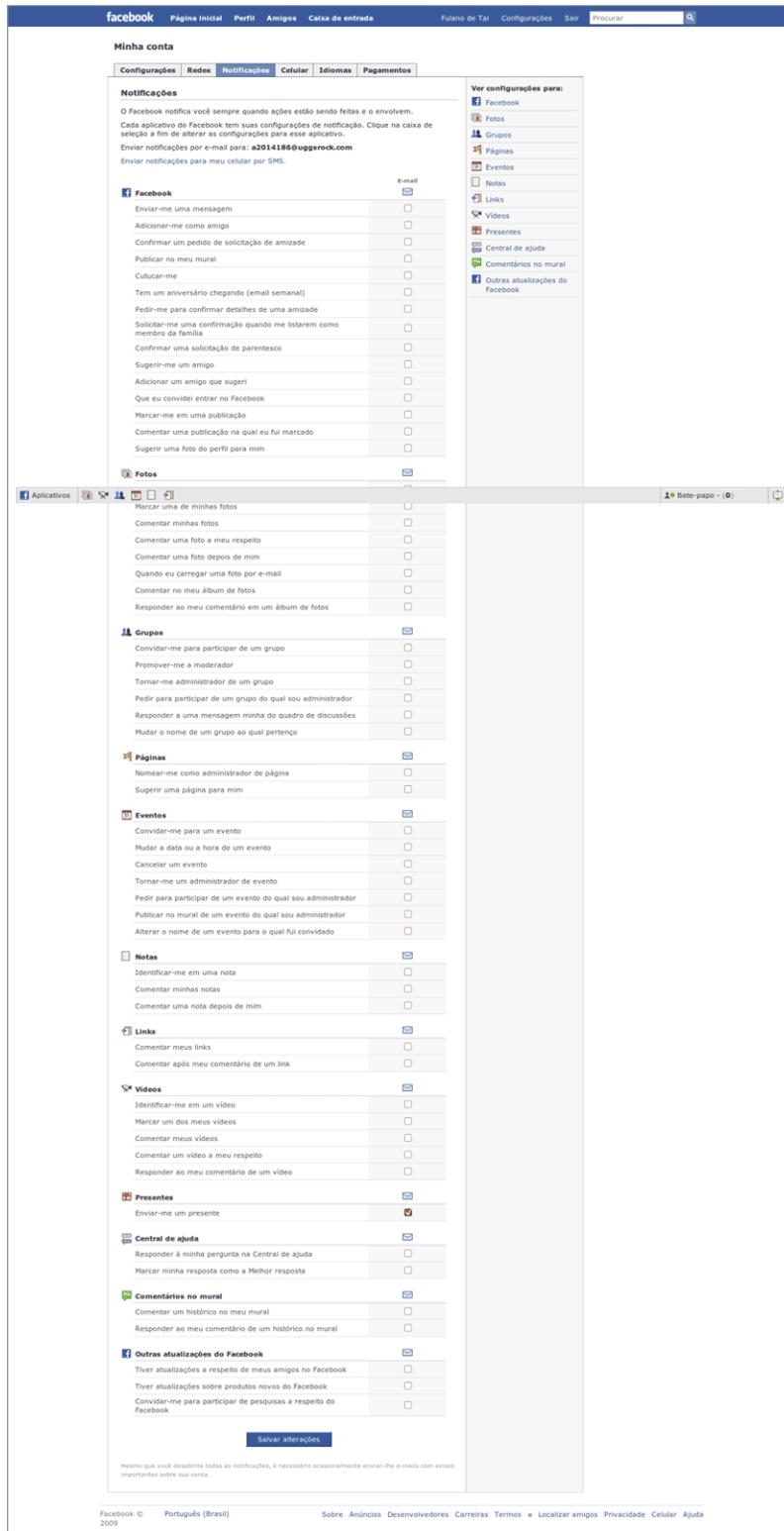


figura 21



Realização



Ministério da
Educação

Ministério da
Ciência e Tecnologia

