



Linked  in

SEGURANÇA

NAS REDES SOCIAIS



CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA
PÚBLICA E DEFESA SOCIAL

EXPEDIENTE CARTILHA SEGURANÇA NAS REDES SOCIAIS

GOVERNADOR DO ESTADO DO CEARÁ

Camilo Sobreira de Santana

SECRETÁRIO DA SEGURANÇA PÚBLICA E DEFESA SOCIAL (SSPDS/CE)

Sandro Luciano Caron de Moraes

SUPERINTENDENTE DE PESQUISA E ESTRATÉGIA DE SEGURANÇA PÚBLICA (Supesp/CE)

José Helano Matos Nogueira

DIRETOR DE ESTRATÉGIA EM SEGURANÇA PÚBLICA (Diesp/Supesp)

Anderson Duarte Barboza

DIRETORA DE PESQUISA E AVALIAÇÃO DE POLÍTICAS DE SEGURANÇA PÚBLICA (Dipas/Supesp)

Manuela Chaves Loureiro Cândido

GERENTE DE ESTATÍSTICA E GEOPROCESSAMENTO (Geesp/Supesp)

Franklin de Sousa Torres

AUTOR

José Helano Matos Nogueira

DESIGNER

Juliana Mendes Teixeira de Lima

REVISÃO

Ascom/Supesp



LINKEDIN (fonte: <https://www.linkedin.com/help/linkedin?lang=pt>)

O **LinkedIn** é a maior rede de relacionamentos profissionais do mundo. Através da sua lista de contatos você pode criar ou manter relações com empresas, colegas de trabalho, mantendo seu *networking*, além de criar currículo *online*, permitindo a procura por empregos e desenvolvimento de carreira.

RISCOS

■ Principais tipos de golpe

- **Golpes fraudulentos relacionados a heranças ou taxas pagas antecipadamente.** esses golpes geralmente solicitam o pagamento adiantado de uma pequena taxa para o recebimento de uma grande quantia em dinheiro.
- **Golpes de oferta de emprego.** esses golpes de oferta de trabalho geralmente envolvem pessoas que se passam por recrutadores ou empregadores que oferecem empregos com altos salários por pouco trabalho.
- **Solicitações financeiras.** não forneça pagamentos ou dados de contas como parte do processo de candidatura. Empresas legítimas não exigem transferências, cheques ou qualquer pagamento como condição para o processo de candidatura.
- **Promessas de remuneração.** uma publicação que destaque o valor do pagamento que você receberá no primeiro ano como adiantamento ou como bônus por assinar.

- **Erros gramaticais.** publicações que incluem vários erros ortográficos e gramaticais.

- **Impostores.** publicações que espelham uma empresa com boa reputação, mas não há *link* para a empresa, os domínios não coincidem ou há dificuldade para localizar um endereço, número de telefone comercial e/ou endereço de e-mail.

- **Anonimidade geral.** prossiga com cautela se não conseguir conferir rapidamente a identidade do anunciante. Um modo de confirmar a identidade é utilizar um mecanismo de pesquisa como Google para verificar os fatos.

- **Golpes de suporte técnico.** não oferecer um número de telefone para suporte ao cliente. Alguns sites anunciam suporte telefônico para o LinkedIn com custo. Esses sites não são afiliados ao LinkedIn. O **LinkedIn** cobra por suporte ao cliente e jamais pede sua senha ou acesso ao seu computador.

- Se você for vítima de um golpe, denuncie-o à polícia local.

- Se você receber uma mensagem de golpe no **LinkedIn**, entre em contato no link disponível em

[https://www.linkedin.com/help/linkedin/ask/TS-RPS:](https://www.linkedin.com/help/linkedin/ask/TS-RPS)

- 1** Identificar a **URL** do perfil do remetente

- 2** Copie e cole a **URL** do perfil do remetente

- 3** Observação: A **URL** pode ser encontrada inserindo ‘**LinkedIn**’ + (**Nome e Sobrenome**) na sua ferramenta de busca preferida, ou você pode inserir o nome na caixa de pesquisa do **linkedin.com**.

DICAS GERAIS

- Altere sua senha periodicamente.
- Saia da sua conta após utilizar computadores de uso público.
- Gerencie as configurações de privacidade e informações da sua conta na página "**Configurações e Privacidade.**"
- Não apresente o seu e-mail, endereço postal ou telefone no "**Resumo**" do seu perfil.
- Conecte-se apenas com pessoas que você conhece e em quem confia ou pessoas com as quais tenha conexões confiáveis.
- Você também pode ativar a verificação em duas etapas na sua conta.
- Obtenha mais informações sobre como denunciar conteúdo inadequado ou preocupações com a segurança.

VISIBILIDADE DO PERFIL

- Seu perfil público exibe uma versão simplificada do seu perfil do **LinkedIn**. Você pode personalizar as suas configurações de perfil para definir quais informações do perfil poderão ser exibidas. Para isso, basta ativar ou desativar as seções de perfil que deseja tornar visíveis em ferramentas públicas de pesquisa.
- O perfil público também é visível para pessoas que não são usuários do **LinkedIn**.

PARA MOSTRAR OU PERSONALIZAR O SEU PERFIL PÚBLICO

- 1 Toque na imagem do perfil > "**Ver Perfil**".
- 2 Toque no ícone  "**Configurações.**"»
- 3 Toque em **Privacidade** > **Edite seu perfil público.**

4 Na seção "**Editar Visibilidade**", use as alternâncias "**mostrar/ocultar**" para selecionar quais seções de perfil você deseja exibir ou ocultar do seu perfil público.

VERIFICAÇÃO EM DUAS ETAPAS

1 **LinkedIn** oferece aos usuários a possibilidade de ativar a verificação em duas etapas das suas contas, o que exigirá a senha da conta e um número de verificação enviado por SMS para o seu celular sempre que não for reconhecido o dispositivo do qual se tenta acessar a conta.

2 Para ativar ou desativar a verificação em duas etapas:

I Toque na imagem do perfil > "**Ver Perfil.**"

II Toque no ícone  **Configurações** no canto superior direito.

III Toque em "**Verificação em duas etapas.**"

IV Toque no botão para habilitar ou desabilitar a verificação em duas etapas.

3 A verificação em duas etapas também pode ser realizada baseada em um telefone compatível com um aplicativo de autenticação como o **Microsoft Authenticator**.

PHISHING

■ Fraudadores podem usar uma prática denominada **Phishing** para obter dados confidenciais, como nomes de usuários, senhas e informações de cartões de crédito. Esses fraudadores se passam por pessoas ou empresas legítimas e enviam e-mails e links, que tentam direcionar você a sites fraudulentos ou infectar seu computador com *malware*.

■ **LinkedIn** nunca perguntará a sua senha ou pedirá que você baixe programas.

POSSÍVEIS SINAIS DE AVISO DE UMA MENSAGEM DE PHISHING

- Contêm erros de ortografia e gramática e que não são endereçadas pessoalmente a você.
- Pedem que você execute alguma ação imediatamente.
- Pedem que você abra um anexo para instalar uma atualização de *software*.

PROTEGENDO-SE DE MENSAGENS FRAUDULENTAS E PHISHING

- Não compartilhe suas informações pessoais, como números de RGs, CPFs, data de nascimento, cartão de crédito ou números de contas bancárias com pessoas que você não conhece.
- Não digite nomes de usuários, senhas ou outras informações pessoais solicitados em *links* de e-mails. É sempre melhor ir diretamente ao site digitando o endereço no navegador.
- Quando se candidatar a empregos na Internet, tenha cuidado com recrutadores que pedem o envio de informações para um endereço de e-mail não associado à empresa. O domínio do e-mail deve conter o nome da empresa como @linkedin.com.
- Tenha cuidado ao clicar em *links* inseridos em mensagens. *Malwares* podem invadir seu sistema caso você clique em um *link* malicioso. Caso suspeite de algo, mova o cursor sobre qualquer *link* (sem clicar nele) para verificar se ele está direcionado para o site real. Para denunciar e-mails de *Phishing* recebidos, encaminhe o e-mail suspeito para phishing@linkedin.com.

■ Se receber uma mensagem no **LinkedIn** e acreditar que é uma tentativa de Phishing, você pode denunciá-la, clicando no ícone.

- É *spam* ou *scam*
- É *scam*, *phishing* ou *malware*

BLOQUEIO DE USUÁRIO

■ Você pode bloquear um usuário para que ele não veja o seu perfil usando o computador ou um dispositivo móvel. Depois de bloquear um usuário, ele será exibido na sua lista de pessoas bloqueadas. O usuário bloqueado não será notificado da sua ação.

PARA BLOQUEAR O ACESSO DE UM USUÁRIO AO SEU PERFIL

- 1** Vá para o perfil do usuário que deseja bloquear.
- 2** Toque no ícone  "**Mais**" no canto superior direito da tela.
- 3** Toque em  "**Denunciar/Bloquear**" no menu suspenso.
- 4** Toque em "**Bloquear**" [nome do usuário].
- 5** Na janela *pop-up* de confirmação, toque em *Bloquear*.

DENÚNCIA

■ Se você tiver alguma preocupação sobre uso inapropriado ou inseguro do **LinkedIn**, existe uma forma de marcar o conteúdo diretamente no site.

DENUNCIAR UMA CONVERSA

- 1** Clique no ícone  **Mensagens** no topo da página inicial do **LinkedIn**.
- 2** Selecione a mensagem na lista da lateral esquerda.
- 3** Clique no ícone  "**Mais**" no canto superior direito da conversa e selecione  **Denunciar esta conversa**.

4 Selecione o motivo apropriado no menu “**Por que você está denunciando isto?**” e siga as instruções apresentadas na tela.

5 Clique em **Enviar** para prosseguir com a denúncia da conversa ou em “**Voltar**” para rever as suas opções.

DENUNCIAR UMA PUBLICAÇÃO OU COMENTÁRIO

1 Clique no ícone  “**Mais**” no canto direito da publicação na página inicial do **LinkedIn**.

2 Clique em  “**Denunciar**” esta publicação.

3 Selecione o motivo apropriado no menu “**Por que você está denunciando isso?**” e siga as instruções apresentadas na tela.

4 Clique em “**Enviar**” para prosseguir com a denúncia da publicação, ou em “**Voltar**” para rever as suas opções.

DENUNCIAR ALGUÉM QUE VOCÊ NÃO CONHECE

1 Clique no ícone  “**Minha rede**” na parte superior da sua página inicial do **LinkedIn**.

2 Clique em **Ignorar** para remover o convite sem aceitá-lo.

3 Clique em “**Eu não conheço esta pessoa**” na janela *pop-up* no canto inferior esquerdo da tela.

DENUNCIAR UM PERFIL FALSO, QUE SE PASSA POR OUTRA PESSOA OU QUE VIOLA OS TERMOS DE USO

- 1** Vá para o perfil que deseja denunciar.
- 2** Clique no ícone  "Mais" e selecione "Denunciar/Bloquear."
- 3** Selecione a ação apropriada na janela *pop-up* "O que você deseja fazer?" e siga as instruções apresentadas na tela.
- 4** Clique em **Enviar** para prosseguir com a denúncia da atualização ou em "**Voltar**" para rever suas opções.

DENUNCIAR PERFIL FALSO

É possível marcar perfis inadequados ou falsos no **LinkedIn** como perfis que contenham palavras abusivas, perfis vazios com nomes falsos ou perfis que utilizem a identidade de pessoas públicas.

- 1** Clique no ícone de  "Mais" no perfil do usuário.
- 2** Clique em  "Denunciar/bloquear."
- 3** Selecione "Denunciar" este perfil na janela *pop-up* "O que você deseja fazer?"
- 4** Na janela *pop-up* forneça mais algumas informações, selecione o motivo apropriado por marcar o perfil.
- 5** Clique em "**Enviar**" para prosseguir, ou em "**Voltar**" para revisar suas opções.

REALIZAÇÃO:



CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA
PÚBLICA E DEFESA SOCIAL