MANUAL DE CUIDADOS DIGITAIS

PARA TRANSATIVISTAS E ALIADES

Expediente

Instituto Brasileiro de Transmasculinidades - Núcleo São Paulo

Coordenação
Kyem Ferreiro

Fomento
Ação Educativa
Artigo 19 Brasil e América do Sul

Autoria
Instituto Brasileiro de Transmasculinidades - Núcleo São Paulo
Rede Transfeminista de Cuidados Digitais
Pajubá Tech
Spectra

Projeto gráfico e diagramação
Pedro Lucas Silvério
Renato Camps

2026
São Paulo

ÍNDICE

OLÁ,
PESSOA LEITORA

Esperamos que você esteja bem, seja no online ou no offline. Te damos boas-vindas ao Manual de Cuidados Digitais para Transativistas e Aliades, criado para oferecer orientações e ferramentas que fortalecem nossa segurança e autonomia em um mundo cada vez mais digital.

Este material é uma construção coletiva do **Instituto Brasileiro de Transmasculinidades – Núcleo São Paulo (IBRAT SP)**, em parceria com a **Pajubá Tech**, a **Rede Transfeminista de Cuidados Digitais** e a **SPECTRA**, com o apoio da **Ação Educativa**, através do Edital 'No Corre!' e **Artigo 19 Brasil e América do Sul**. Nosso objetivo é democratizar o acesso à informação e contribuir para a criação de ambientes digitais mais seguros para pessoas trans e aliades

Neste primeiro episódio, queremos contar um pouco como este projeto nasceu da força da nossa própria comunidade.

A ideia surgiu durante a Assembleia da 2ª Marcha Transmasculina de São Paulo, a primeira marcha transmasculina do Brasil e do mundo. Essa assembleia, fruto de um chamamento popular, reuniu diversas vozes comprometidas com a construção da marcha. Durante o encontro, muitas pessoas levantaram dúvidas e preocupações sobre como se proteger de ataques e assédios virtuais, como cuidar da própria imagem, das informações pessoais, e como se sentir mais seguras nas redes, afinal tanto a divulgação quanto a publicação dos registros da marcha são no ambiente digital.

Foto: Walison Matos| 2ª Marcha Transmasculina de São Paulo, 2025

No dia **30 de março de 2025**, mais de 7 mil pessoas ocuparam a Avenida Paulista na Marcha Transmasculina, reivindicando visibilidade, direitos e dignidade para nossa população. Porém, logo após o evento, alguns participantes e apoiadores foram alvo de diferentes formas de exposição digital, o que reforçou a urgência de pensar coletivamente estratégias de proteção. Foi a partir dessa experiência que entendemos:

NAVEGAR COM SEGURANÇA TAMBÉM É UM ATO DE RESISTÊNCIA.

Por isso, em maio de 2025 fizemos uma oficina de Cuidados Digitais para Transativistas e Aliades, que aconteceu na CryptoRave em parceria com Rede Transfeminista de Cuidados Digitais e agora, lançamos este manual como um instrumento de cuidado, autonomia e fortalecimento comunitário.

Afinal, ainda que muitas vezes pareça que a internet não é um espaço de direitos para pessoas trans e aliades, ela é e deve ser. Mas, você deve estar se perguntando se há um tipo de "Constituição Digital", né?

→ Durante muito tempo, a internet foi um território sem regras claras e um espaço em que princípios, garantias, direitos e deveres praticamente não existiam. Isso mudou em 2014, com a criação do Marco Civilda internet, conhecido como a "Constituição Digital Brasileira".

Antes dessa lei, não havia regulamentação específica sobre o uso da internet no país. Questões como liberdade de expressão, invasão de privacidade e proteção de dados pessoais eram tratadas apenas com base na Constituição Federal, o que deixava muitas lacunas e incertezas jurídicas.

E você pode estar se perguntando:

"O QUE O MARCO CIVIL DA INTERNET TEM A VER COM CUIDADOS DIGITAIS?"

A resposta é: **TUDO!**

Enter ↵

Foto: Site Folha de São Paulo

Foi a partir dele que princípios como a

- **LIBERDADE DE EXPRESSÃO**
- **PRIVACIDADE**
- **PROTEÇÃO DE DADOS PESSOAIS**

passaram a ser **reconhecidos e garantidos por lei** para a construção das bases para um ambiente digital mais seguro, transparente e inclusivo.

Esse marco legal garante que tenhamos maior controle sobre nossas informações online e, caso sejamos vítimas de crimes digitais, temos o direito de denunciar, exigir investigação e cobrar que os autores sejam responsabilizados.

O Marco Civil é, portanto, uma ferramenta de defesa dos nossos direitos digitais e conhecê-lo é o primeiro passo para navegar com segurança e consciência, especialmente em tempos de desinformação, ataques virtuais e discursos de ódio.

PROTEÇÃO DE CONTAS

Protegendo nossas contas e espaços digitais

O roubo de contas de redes sociais ou o acesso indevido a e-mails são **ataques muito comuns** e geralmente utilizados com o objetivo de realizar fraudes e aplicar golpes financeiros. No contexto das comunidades trans e travesti, no entanto, além das motivações financeiras, essas estratégias podem ser utilizadas como **forma de exposição não consentida, silenciamento e intimidação**.

Ao invadir uma conta, a pessoa agressora pode apagar conteúdos, acessar conversas íntimas, divulgar informações pessoais ou se passar pela vítima, colocando em risco sua segurança pessoal, sua reputação, e causando danos emocionais profundos. O vazamento de informações pessoais pode, também, facilitar e estimular novas agressões, gerando ondas de discursos de ódio, abusos e ameaças.

O impacto desses ataques pode se estender para além de um único indivíduo, alcançando redes e movimentos inteiros, colocando outras pessoas em risco ou desorganizando ações coletivas. Proteger nossas contas é um passo importante para preservar nossa integridade, mas também diz respeito a uma proteção coletiva, uma vez que estamos protegendo não só nossas informações, mas também as trocas, redes e articulações que construímos com outras pessoas. Por isso, segurança digital não é só uma questão individual, é uma prática de cuidado mútuo, uma forma de manter vivas e seguras as conexões que sustentam nossas lutas e afetos.

Perder uma conta ou ter um perfil invadido pode ser traumático, mas medidas preventivas simples podem fazer toda a diferença. Para começar, precisamos saber antes quais estratégias e pontos fracos podem ser usados contra nós para roubar e invadir nossas contas.

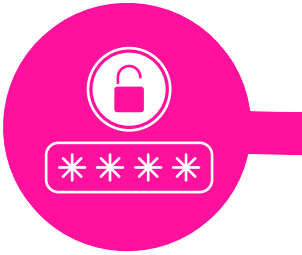
O QUE PODE SER USADO CONTRA NÓS?

Engenharia social e Phishing

Engenharia social é uma forma de manipulação psicológica em que a pessoa é enganada a realizar ações ou revelar informações confidenciais. Um exemplo comum é o phishing, ataque onde a pessoa tenta obter informações confidenciais (como senhas, dados bancários, etc) ao se apresentar como uma pessoa ou instituição confiável através de e-mail, SMS, mensagem ou telefonema. O termo "phishing" vem da palavra inglês “fishing”, pescar, e refere-se ao uso de iscas para "pescar" informações. Um exemplo típico são mensagens que se passam por alguma instituição financeira, com tom urgente, pedindo que você clique em um link para, por exemplo, ‘verificar uma transação’. Esses links levam a páginas falsas feitas para roubar dados. Muitas vezes, a vítima só percebe o golpe depois que seus dados já foram usados indevidamente. Há alguns anos, esse tipo de ataque foi usado para roubar diversas contas de coletivos ativistas brasileiros no Instagram.

Força bruta para “quebrar” senhas

O ataque de força bruta é um método utilizado para descobrir uma senha a partir de tentativa e erro. A pessoa atacante testa todas as combinações possíveis para uma senha, até descobrir a correta. Essas tentativas também podem ser automatizadas e alimentadas com informações de contexto ou com dados pessoais da vítima (nomes de pessoas da família, datas de aniversários), além de dicionários de palavras em diversos idiomas, o que acelera muito o processo. No entanto, alguns dos serviços que mais utilizamos (como o Gmail, por exemplo) já possuem proteções contra esse tipo de ataque, como limite de tentativas com bloqueios temporários, etc.



Vazamento de banco de dados

Vazamento de banco de dados ocorre quando informações armazenadas por empresas e serviços (logins, e-mails, senhas, documentos) são expostas por falhas de segurança da própria empresa/serviço. Esses dados podem ser vendidos em mercados ilícitos, usados para fraudes ou para facilitar phishing e ataques de engenharia social. Para checar se suas contas já caíram em vazamentos, vá até o site https://haveibeenpwned.com/ e teste os emails que costuma utilizar para criar contas em serviços.

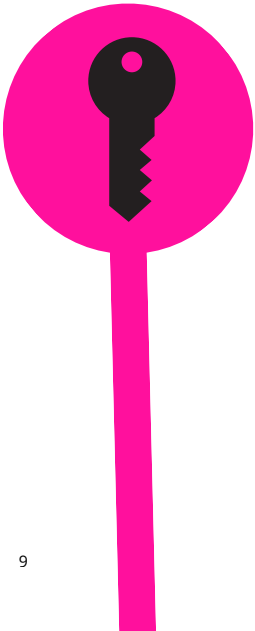
Mau gerenciamento de senhas

A chave do tesouro é o tesouro! Senhas mal armazenadas e mal gerenciadas colocam em risco nossos dados. Exemplos de senhas mal armazenadas são senhas escritas em post-its e mantidas perto do computador e senhas armazenadas em bloco de notas no celular, ou enviadas por email, que podem ser facilmente acessadas, por exemplo, quando roubam nosso celular.

BOAS PRÁTICAS PARA NOS MANTER SEGURES

Diante desse cenário, há algumas coisas que podemos fazer para proteger nossas contas, entre elas:

Criar senhas fortes

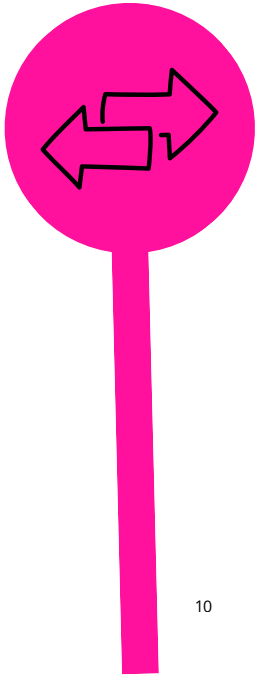


Senhas longas com 6 ou mais caracteres. Quanto maior e mais mistura de palavras e línguas diferentes, dialetos e gírias, mais difícil será de decifrar a sua senha. Use a criatividade, **misture inglês, português, yorubá, pajubá, línguas indígenas, números, caracteres especiais.** No site https://www.security.org/how-secure-is-my-password/ você pode ter uma ideia de quão frágil é a sua senha. Mas cuidado, o site deve ser utilizado de forma lúdica, e também não coloque lá sua senha real, coloque algo parecido, uma senha com a mesma estrutura e número de caracteres, por exemplo.

Não crie senhas com dados pessoais.
Não use datas de aniversário, endereço, nome de parentes ou de bichos de estimação. E**sse tipo de informação pode ser facilmente obtida através de vazamento de dados**, de uma análise atenta de suas redes sociais ou de pesquisas sobre você na Internet.

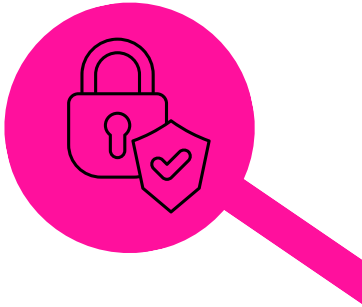
Use senhas diferentes para cada serviço.
Se alguém descobrir a sua senha, seja por engenharia social, phishing ou vazamento de banco de dados, **ela poderá acessar diversas contas suas de uma só vez**, e causar um belo estrago na sua vida.

Troque suas senhas com regularidade.
Acredite, vazamentos de bancos de dados acontecem o tempo inteiro, mesmo em serviços populares, deixando senhas e contas expostas. Trocar de senha a cada 6 meses pode ser uma boa, ou sempre que desconfiar que a senha foi comprometida, principalmente em serviços em que você não tenha configurado múltiplos fatores de autenticação. Para confirmar se a senha de algum serviço que você usa foi comprometida, visite: haveibeenpwned.com (site em inglês). Através desse site você consegue identificar vazamentos de dados a partir de um e-mail específico.



Configurar múltiplos fatores de autenticação

É um método de autenticação que exige uma combinação de coisas para que seja realizada a identificação e a liberação do acesso à conta. Fatores de autenticação geralmente são uma coisa que você tem conhecimento (ex. uma senha), e uma coisa que você possui (ex. número de telefone, aplicativo de autenticação). É como se você adicionasse um portão a mais para acessar sua conta. No primeiro portão você apresenta uma forma de autenticação, como por exemplo uma senha, no segundo portão você apresenta outra, como por exemplo um número de telefone para receber um código via sms. Grande parte dos serviços digitais que utilizamos hoje em dia possuem essa possibilidade, e é muito importante configurá-la.



Utilizar um gerenciador de senhas e um gerador

Se você vai criar senhas complexas, longas, e vai ter uma senha para cada serviço, vai ser impossível memorizar todas elas. Por isso é importante utilizar um gerenciador de senhas, como o KeepassXC ou Bitwarden. Com eles, é possível guardar e organizar logins e senhas de forma criptografada, e você só precisará lembrar de uma senha, a que abre o gerenciador. Os gerenciadores também vêm equipados com um gerador de senhas, que cria senhas aleatórias, misturando diferentes tipos de caracteres.

Ter cuidado onde clica

Ao receber e-mails, SMS ou mensagens privadas, desconfie do tom de urgência; analise bem a mensagem escrita e procure erros; analise o endereço do remetente e o link enviado, e veja se corresponde a endereços oficiais e confiáveis. Evite clicar em links suspeitos ou baixar anexos inesperados. Sempre que possível, confirme a informação diretamente com a instituição ou pessoa que supostamente enviou a mensagem, usando canais oficiais.

E O QUE FAZER EM CASO DE ROUBO OU INVASÃO DE CONTAS?

Enter ↵

Altere suas senhas imediatamente

Caso ainda tenha acesso a conta, troque a senha imediatamente e construa uma senha forte e exclusiva. Se você utiliza a mesma senha comprometida para outros acessos, troque a senha também. Nesses casos, sugerimos que ative a autenticação em dois fatores (2FA) para obter uma proteção extra.

Tente recuperar o acesso

Caso a pessoa invasora tenha trocado a senha ou as credenciais de acesso à conta, tente recuperar o acesso através de opções como “Esqueci a senha”, e utilize seu email de recuperação, telefone, códigos de segurança ou perguntas de segurança para redefinir a senha.

Caso a pessoa invasora tenha alterado também o email ou telefone de recuperação ou o segundo fator de autenticação, procure uma opção do tipo “Não consigo acessar este email/número de recuperação”, ou “Minha conta foi invadida”, muitos sites têm um formulário específico para esses casos.

Verifique atividades recentes

- Revise os dispositivos conectados e sessões ativas (geralmente nas configurações de segurança da conta), e revogue o acesso desconectando qualquer login suspeito.
- Revise e revogue também aplicativos e extensões conectados à conta, caso algum seja suspeito.
- Veja se há mensagens, postagens ou links enviados sem seu consentimento.
- Informe amigues, familiares e contatos profissionais sobre a invasão da conta, e oriente para que não cliquem em links suspeitos enviados através da sua conta.

Peça ajuda!

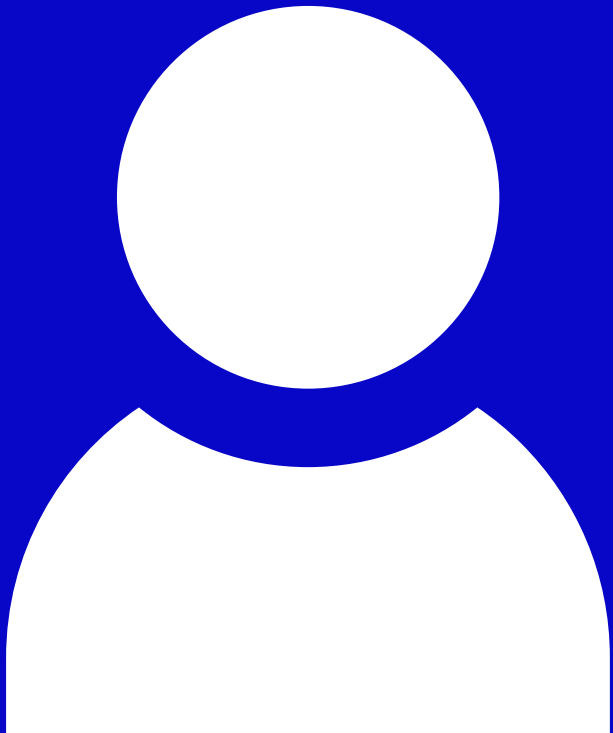
Se não se sentir confortável em tomar as medidas, ou não tenha conseguido retomar sua conta, entre em contato com linhas de ajuda de cuidados digitais e peça ajuda:

Maria D'ajuda
Linha de ajuda feminista brasileira
https://mariadajuda.org/

Access Now
Linha de ajuda internacional
https://www.accessnow.org/help/

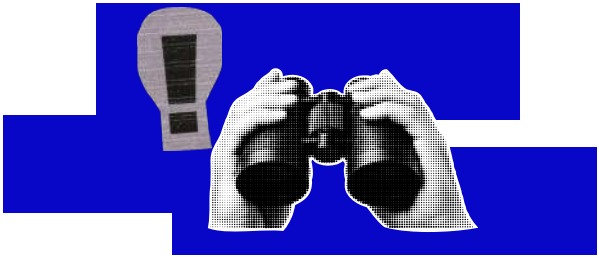
DOXXING E OUTING

Protegendo sua identidade



Doxxing é quando alguém **expõe seus dados pessoais na internet sem seu consentimento** como telefone, e-mail, endereço, etc. Para pessoas trans e travestis, essa prática se torna ainda mais cruel com o outing, que é a **exposição da nossa identidade trans e o uso do nosso antigo nome para nos atacar**. Um exemplo drástico é quando cruzam nosso nome social ou retificado, com o nome antigo e CPF, expondo toda a nossa vida burocrática e nos forçando a reviver um passado que lutamos para superar.

Esta seção vai te ensinar a procurar e apagar os rastros que você considera sensíveis ou que não deseja que estejam online, e a criar uma fortaleza digital para proteger quem você é.



Mapeamento de dados (Self-Doxxing)

O primeiro passo para se proteger é **entender o que já está disponível sobre você online**. Isso inclui informações pessoais, fotos antigas, endereços, e até perfis esquecidos. O objetivo é descobrir o que agressores poderiam encontrar e agir antes que isso aconteça.

A seguir, veja como fazer seu próprio mapeamento de dados, pesquisando seu nome antigo e outros termos relacionados. Antes de começar, no entanto, saiba que esse processo pode assustar, trazer ansiedade e medo.

Nesse caso, **reserve um tempo para fazer o mapeamento com calma e foco**. Também sugerimos que **peça a ajuda de amigues** para acompanharem o processo, mas pode ser legal também **utilizar as estratégias que você já tem para ficar calme, ou seja, exercícios de respiração, meditação, tomar um chá, etc.**

Para uma busca exata, use aspas.

Isso força o site de busca a procurar exatamente por aquele nome.

"Nome Sobrenome Antigo"

Para buscar em um site específico, use site:

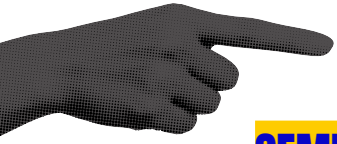
É perfeito para procurar dentro de uma rede social antiga ou site da faculdade.

"Nome Antigo" site:facebook.com

Para encontrar documentos, use filetype:

Ótimo para achar seu nome em PDFs de listas de vestibular, artigos ou editais.

"Nome Antigo" filetype:pdf



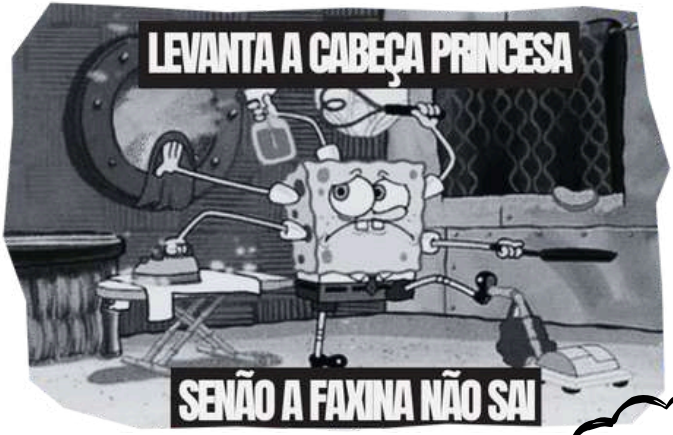
DICA DE OURO

SEMPRE FAÇA ESSA BUSCA EM UMA JANELA ANÔNIMA DO SEU NAVEGADOR.

Isso evita que os navegadores usem nosso histórico pessoal e te mostre resultados mais parecidos com o que um estranho veria.

DEPOIS DE MAPEAR SEUS RASTROS, É HORA DA LIMPEZA

O cuidado digital não é só apagar o passado, mas construir um futuro mais seguro.



Aqui está um checklist prático para começar

FAÇA O SEU CHECK!

- [ ] **Apague contas que não usa mais.**
  Sites como o **JustDelete.me** te dão o link direto para a página de exclusão de centenas de serviços, o que facilita muito!

- [ ] **Exija seu direito de ter seus dados apagados.**
  A Lei Geral de Proteção de Dados (LGPD) está do nosso lado. Você pode e deve exigir que sites e empresas apaguem suas informações antigas.

- [ ] **Crie e-mails "descartáveis".**
  Tenha um e-mail secundário apenas para se cadastrar em lojas, aplicativos e promoções. Mantenha seu e-mail principal seguro e privado.

Use uma chave aleatória como sua chave Pix.

Recomendamos que sua chave pix seja aleatória, pois dados como seu e-mail, telefone e até CPF, em alguns casos, são informados a outras pessoas sem seu consentimento. Isso pode expor seus dados pessoais e sensíveis como seu nome antigo, por exemplo.

MODELO "COPIA E COLA" PARA ACIONAR A LGPD

Nova mensagem

Para: E-mail do site onde encontrou seus dados

Assunto: Solicitação de Remoção de Dados Pessoais (LGPD)

"Espero que esse e-mail encontre todes bem.
Meu nome social é [Seu Nome Social] e escrevo para solicitar a remoção de dados pessoais antigos, sob o nome [Seu Antigo Nome de Registro], que encontrei no link: [Cole o link exato aqui].

Com base na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), exerço meu direito à eliminação dos dados do seu banco de dados. Solicito a remoção completa e imediata destas informações do seu sistema e aguardo uma resposta em até 15 dias.

Atenciosamente,
[Seu Nome Social]."

Aa

Enviar

CAMINHOS PARA A CONTENÇÃO DE DANOS

O que fazer APÓS um vazamento

Se seus dados vazarem, aja rápido para conter os dados. Identifique o que vazou e siga o protocolo correspondente.

1. **Mude a Senha da "Conta-Mãe" PRIMEIRO:** Sua prioridade é seu e-mail de recuperação. Troque a senha dele antes de todas as outras.
2. **Troque Senhas Críticas:** Altere imediatamente as senhas do seu e-mail principal, redes sociais e contas bancárias.
3. **Ative a Autenticação de Dois Fatores (2FA):** Ative o 2FA em todas as contas, de preferência com um app autenticador (ex: Authy, Aegis), não por SMS.
4. **Desconecte Estranhos:** Nas configurações de segurança (Google, Instagram, etc.), procure por "Dispositivos Conectados" e remova qualquer sessão que não reconheça.

Se vazaram seus DADOS PESSOAIS (Doxxing)

O foco é sua segurança física e financeira.

1. **Alerte sua Rede Imediata:** Avise familiares e pessoas que moram com você sobre o vazamento do seu endereço e para desconfiarem de ligações ou visitas estranhas.
2. **Proteja seu Telefone (SIM Swap):** Ligue para sua operadora e peça para bloquear a troca de chip (SIM Swap) sem sua presença ou senha de segurança. Isso impede que roubem seu WhatsApp e contas de banco.
3. **Monitore seu CPF:** Use o serviço “Registrato” (do Banco Central) para verificar se abriram contas ou empréstimos no seu nome.
4. **Avise seu Trabalho/Estudo:** Informe o RH ou coordenação para que fiquem alertas a tentativas de golpes usando seus dados.

Se ocorreu EXPOSIÇÃO DE IDENTIDADE (Outing)

O foco é controlar a narrativa e proteger sua saúde mental.

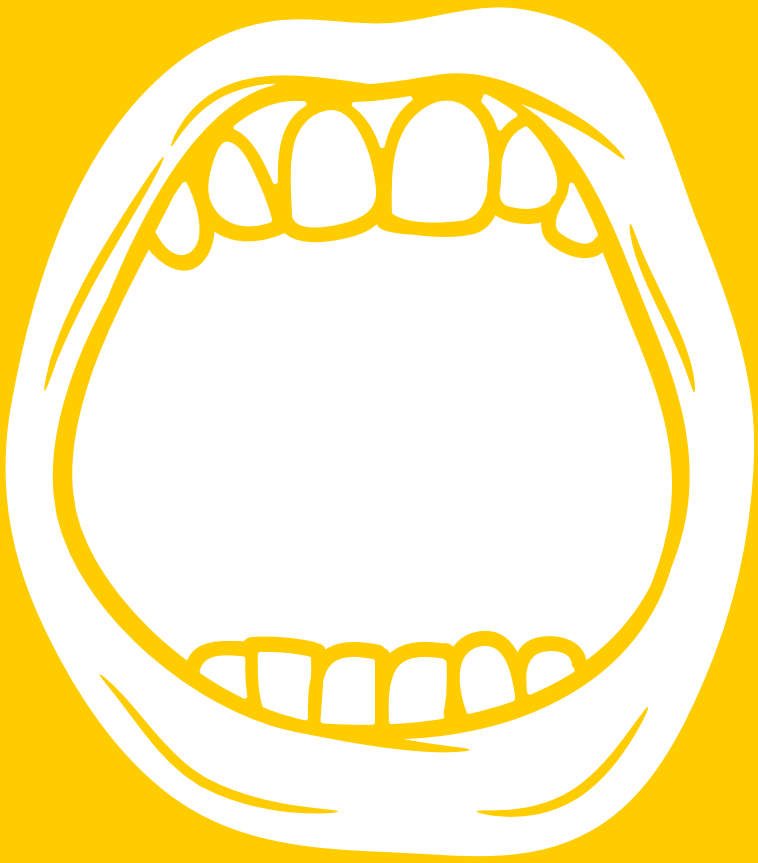
- **Controle a Narrativa (Se for seguro):** Avise sua rede de confiança (amigues, RH) sobre o que aconteceu, explicando que você foi vítime de um ataque.
- **Tranque as Redes:** Mude seus perfis para "Privado" por um tempo para limitar o fluxo de novos ataques.
- **Execute o Protocolo de "Assédio":** O outing é um assédio. Ative o protocolo da seção "Assédio": documente tudo (prints perfeitos), denuncie e bloqueie.

O ataque passou, mas a vigilância continua

1. **Crie Alertas:** Use o Google Alertas para monitorar seu nome social, nome de registro e CPF.
2. **Monitore Senhas:** Cadastre seu e-mail no Have I Been Pwned? para saber de novos vazamentos.
3. **Reforce a Limpeza:** Volte à seção de "Higiene Digital" e execute o protocolo de remoção de dados via LGPD.

ASSÉDIO:

Protocolo de autodefesa



Se você está sofrendo um **ataque online**, a primeira coisa a saber é:

A CULPA NÃO É SUA!

A segunda é que você pode e deve reagir de forma segura e estratégica para se proteger e buscar justiça.

O assédio online se configura quando alguém, individualmente ou em grupo, utiliza meios digitais — como redes sociais, mensagens, fóruns ou e-mails — para ofender, humilhar, ameaçar, perseguir, expor, divulgar informações íntimas sem consentimento ou espalhar conteúdo falso sobre você. Ele pode acontecer uma única vez, mas geralmente envolve repetição e intenção de causar dano psicológico, emocional ou reputacional. Nenhum desses comportamentos é aceitável — e todos podem ser denunciados.

Coleta de provas

Quando o assédio acontece, seu primeiro instinto pode ser apagar tudo para não ter que ver mais. **NÃO FAÇA ISSO**. As ofensas e ameaças são as provas do crime, e você vai precisar delas.

REGRA Nº1:
NÃO APAGUE NADA

Respire fundo. Antes de bloquear ou denunciar, documente tudo.

GUIA RÁPIDO DO "PRINT PERFEITO"

Um print feito em casa mesmo que capture a ofensa/ameaça, a identificação do agressor (perfil ou @), endereço da página (URL / Link) e data e hora, **não tem valor legal**. Principalmente porque, hoje em dia, com a presença de inteligências artificiais é muito fácil manipular imagens, criar prints falsos e etc.

Nesse caso, indicamos algumas alternativas:

Faça uma "Ata Notarial".

A ata notarial é um documento público lavrado por um tabelião de notas que certifica, de forma imparcial e autêntica, a ocorrência ou existência de um fato ou situação, servindo como poderosa prova judicial e extrajudicial. Essa é uma opção mais custosa financeiramente falando.

Fazer o print direto na delegacia.

Realizar o print presencialmente direto na delegacia mais próxima, com a presença de um escrivão ou delegado, para dar fé pública à imagem coletada.

Usar aplicativos de verificação.

O aplicativo "Verifact", "OriginalMy" e o mais novo aplicativo lançado pelos cartórios o "e-Not Provas" são plataformas online que coletam e certificam provas digitais com validade jurídica para uso em processos judiciais, simulando uma coleta forense e atuando como alternativa à ata notarial, garantindo a integridade do conteúdo através de um ambiente antifraude patenteado e metadados técnicos, sendo aceita no Judiciário. Os aplicativos são pagos mas vale dar uma olhada nas especificações de cada um para entender se abrange para o que de fato precisa.

DENUNCIA E APOIO

Você agiu. Agora, peça reforço! Com as provas salvas, você não precisa continuar sozinhe. É hora de agir para parar o ataque e buscar sua rede de apoio.

Protocolo pós-ataque

Denuncie na Plataforma: Use a ferramenta de denúncia da própria rede social (Instagram, Twitter/X, TikTok, etc.). Isso cria um registro formal do abuso.

Bloqueie o Agressor: Depois de salvar todas as provas, bloqueie o perfil para cortar o contato e proteger sua saúde mental.

Busque Apoio Jurídico: Com as provas organizadas, procure organizações públicas, da sociedade civil ou coletivos que oferecem suporte legal. Seus prints bem tirados são a ferramenta mais poderosa que você pode entregar para uma pessoa advogada.

Cuide de Você: Ataques online são exaustivos. Fale com amigues de confiança, procure os coletivos que fazem parte deste projeto ou busque apoio psicológico. Sua segurança e bem-estar vêm em primeiro lugar.

Onde buscar apoio

Essas organizações oferecem diferentes tipos de ajuda jurídica, psicológica e técnica para pessoas vítimas de assédio ou violência online:

SaferNet Brasil: Canal de denúncia e orientação gratuita sobre crimes e violações de direitos humanos na internet.
(https://www.safernet.org.br)

Delegacias Especializadas em Crimes Cibernéticos: Presentes em diversos estados, recebem denúncias formais e orientam sobre os próximos passos legais.

Mapa do Acolhimento: Rede que conecta mulheres vítimas de violência a atendimentos psicológicos e jurídicos gratuitos.
(https://mapadoacolhimento.org.br)

Instituto AzMina: Oferece conteúdos e iniciativas de apoio para vítimas de violência de gênero e ataques digitais.
(https://azmina.com.br/)

Núcleos de Prática Jurídica (NPJ): Presentes em faculdades de Direito, oferecem atendimento jurídico gratuito supervisionado.

Ouvidorias de Direitos Humanos (Disque 100): Canal público nacional para denunciar violações de direitos humanos, inclusive assédio e ameaças online.

Acoso.online: Site que reúne informações sobre como resistir e denunciar violência de gênero online.
(https://acoso.online/)

PLUS:

Espera um pouquinho que tem mais coisa ai!

COMO INCLUIR NOME SOCIAL EM SERVIÇOS?

É sabido que umas das práticas de maiores violências e exclusão com pessoas trans e travestis é o desrespeito com o nome social. Por isso, nessa cartilha **separamos um tópico para ajudar você a fazer a inserção do nome social nos seus documentos**.

Desde o **decreto nº 8.727/2016 é assegurado a inclusão, alteração ou exclusão do nome social no seu CPF.** A solicitação pode ser realizada via processo digital acessando o site do gov.br ou presencial em alguma unidade da receita federal próximo da sua casa. Mas para ser atendide você precisa agendar uma data e horário no site do gov.br.
Seja cuidadose nesse processo, esteja certe de acessar o site oficial.

BORA LÁ PARA AS ORIENTAÇÕES PRÁTICAS?

Para começarmos, é necessário que você tenha uma conta no gov.br.
Um documento de identificação oficial, exemplo: RG, CIN, CNH.
E caso seja menor de 16 anos, o documento oficial do seus tutores ou sua/seu tutore.

Siga o passo a passo:

1° Passo: Acesse o site gov.br

2° Passo: Na barra de pesquisa “o que você procura?” escreva “nome social” e em seguida clique em “incluir, alterar ou excluir nome social”, e logo após clique em “iniciar”

3° Passo: Para abrir o processo você deve clicar em “solicitar serviço via processo digital”

4° Passo: Em “Área de Concentração de Serviço” escolha “Cadastro”

5° Passo: Em “Serviço” você deve escolher “CPF - Incluir, alterar ou Excluir Nome Social no CPF para pessoa travesti ou transexual”

6° Passo: Em seguida, junte os documentos necessários para serem enviados.

7° Passo: Enviar e acompanhar o requerimento pelo portal do e-CAC.

O resultado do processo será informado por meio de um despacho acessando a página do processo digital através do gov.br. Atenção para os menores de 16 anos, o seu responsável deve te acompanhar e assinar o requerimento para a inclusão do nome social.

Caso o pedido for por e-mail ou presencial, você precisa preencher o requerimento de “pedido de inclusão, alteração ou exclusão do nome social”. Caso seja via e-mail você vai clicar no painel de canais de prestação e ver os endereços emails de acordo com seu estado.

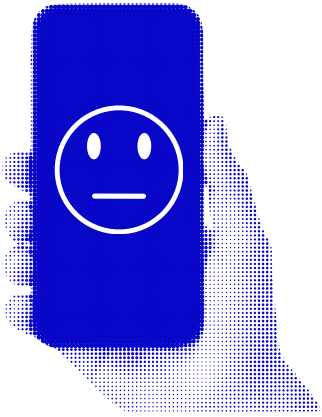
Com a alteração feita no CPF as alterações nos sistemas já devem ser atualizadas automaticamente. Caso não seja, faça uma reclamação junto a ouvidoria pois estão infringindo a portaria cocad n° 65/2024 que operacionaliza a inclusão no sistema da Receita Federal.

AGORA VAMOS TE EXPLICAR SOBRE A CARTEIRA DE IDENTIDADE NACIONAL (CNI)

A Carteira de Identidade Nacional (CIN), dispõe da instrução normativa RFB n° 2.172/2024 que estabelece as regras para inclusão do nome social no CPF. **A primeira emissão da CIN é gratuita** e você pode agendar um atendimento presencial no Instituto de Identificação do seu estado, **acessando o site do governo do seu estado.**

E olha que legal, ela usa o CPF como o número de identificação e tem validade em todo território nacional, mas ainda traz o nome civil e o campo "sexo".

O uso do nome social é garantido em escolas públicas e privadas, conforme a resolução do Conselho Nacional de Educação, caso haja recusa em respeitar o nome social, você pode fazer uma denúncia à Ouvidoria do Ministério da Educação (MEC) ou da Secretaria de Educação do estado/município. Se liga, no **ambiente corporativo**, o uso do nome social é **garantido na administração pública federal** e deve ser respeitado em ambientes privados.



MEU CELULAR FOI FURTADO OU ROUBADO, E AGORA?

Ao ter o celular roubado, os primeiros minutos e horas após o roubo são essenciais para proteger os seus dados.

Aja rapidamente seguindo esses passos:

1. **Em outro dispositivo, acesse sua conta Google ou iCloud.**

Para localizar, proteger, desconectar ou apagar os dados do celular. **Esta ação precisa ser feita o mais rápido possível, já que o celular precisa estar ligado e conectado à Internet para que os comandos funcionem.** É comum que, após o roubo, o celular seja colocado em modo avião ou tenha os dados desligados, por isso agir rápido é essencial.

Para iPhone, siga as instruções pelo link:

https://support.apple.com/pt-br/120837

Para Android, siga as instruções pelo link:

https://support.google.com/accounts/answer/6160491?hl=pt-br#zippy=%2Climpar-redefinir-ou-remover-o-dispositivo

2. **Ligue na operadora e bloqueie o IMEI e o Chip**.
Bloqueando o IMEI você impede que seu celular seja utilizado para se conectar com a rede de telefonia utilizando outro chip, e bloqueando o chip você impede que ele seja utilizado em outro aparelho celular, inclusive para recuperar contas e afins.

3. **Ative sua linha em um novo chip** e, em outro aparelho (novo ou de amigues) faça login nas suas contas de aplicativos de mensagens, como Whatsapp, por exemplo. Com isso você retomará o acesso a sua conta.

4. **Ligue para os bancos** e peça para desconectar o aplicativo. Também avalie e conteste saldos, uso de cartões e pedidos de empréstimo estranhos. Alguns aplicativos, como o NuBank, por exemplo, possuem um serviço específico para roubo e perda de celular. Entre no serviço e desconecte o celular roubado.

5. **Tente lembrar e liste todos os aplicativos instalados no celular nos quais você tem conta, e troque as senhas de todos os serviços**. Priorize as senhas do Google, Apple ID, e-mail, bancos e redes sociais. Ative também a autenticação em dois fatores sempre que possível.

6. **Faça Boletim de Ocorrência,** inclusive adicionando e descrevendo qualquer ocorrência com bancos e cartões. **O B.O. é essencial** para que você se defenda caso um criminoso tente se passar por você depois do furto ou roubo.

Seu celular estava com a tela desbloqueada?

Se o seu celular era um **Android** e você havia ativado a opção **"Bloqueio remoto (Remote Lock)**", acesse o site **https://android.com/lock** imediatamente após o roubo e bloqueie a tela do aparelho para impedir o acesso aos seus dados.

Se o seu celular era um **iPhone**, acesse imediatamente o site **https://www.icloud.com/find** e coloque o aparelho no **"Modo Perdido (Lost Mode)"**. Dessa forma, o iPhone será bloqueado remotamente e impedirá o acesso não autorizado aos seus dados pessoais.

COMPROU UM CELULAR NOVO? PROTEJA SEUS DADOS!

1. **Proteja o celular com senhas.**
Configure uma senha forte (alfanumérica) de bloqueio do celular e, sempre que possível, configure senhas para abrir aplicativos

2. **Proteja seu chip. Configure uma senha/PIN pro seu chip.**
Dessa forma, se tentarem utilizar seu chip em outro aparelho, vão precisar da senha. Ou mesmo se desligarem ou ligarem novamente o aparelho roubado. **Anote e guarde bem essa senha, ou pode correr o risco de não conseguir mais utilizar seu chip.** Para configurar a senha do chip será preciso colocar a senha que vem no cartão no momento em que você compra o chip. Se não

possui mais o cartão, entre em contato com a operadora.

3. **Para celulares Android:** Crie uma conta Google nova para ser configurada e utilizada exclusivamente como a conta vinculada ao seu celular Android. Assim, se alguém tiver acesso ao seu aparelho, poderá acessar apenas essa conta sem movimentação, e não a sua conta pessoal ou de trabalho que guardam inúmeros documentos sensíveis.

4. **Não guarde senhas no bloco de notas ou em qualquer lugar acessível no celular**, **inclusive em contas de e-mail**. Virou uma prática de quem rouba celulares procurar por senhas anotadas, possibilitando o acesso a contas como, por exemplo, de aplicativos de bancos.

5. **Configure a tela de bloqueio** de modo que a opção de "Modo avião" não fique acessível. Dessa forma você impede que a pessoa que roubou o celular desconecte o aparelho da Internet.

6. **Anote e guarde bem o IMEI do celular**. Para descobrir o IMEI, basta discar *#06# no celular.

7. **Faça backups regulares dos dados do seu celular!** Dessa forma, caso fique sem o aparelho, você não perde também a memória de anos de vida.

ACESSE AQUI TODOS OS LINKS CITADOS AO LONGO DO MANUAL

Realização

Fomento

Conteúdo


ibrat
núcleo são paulo