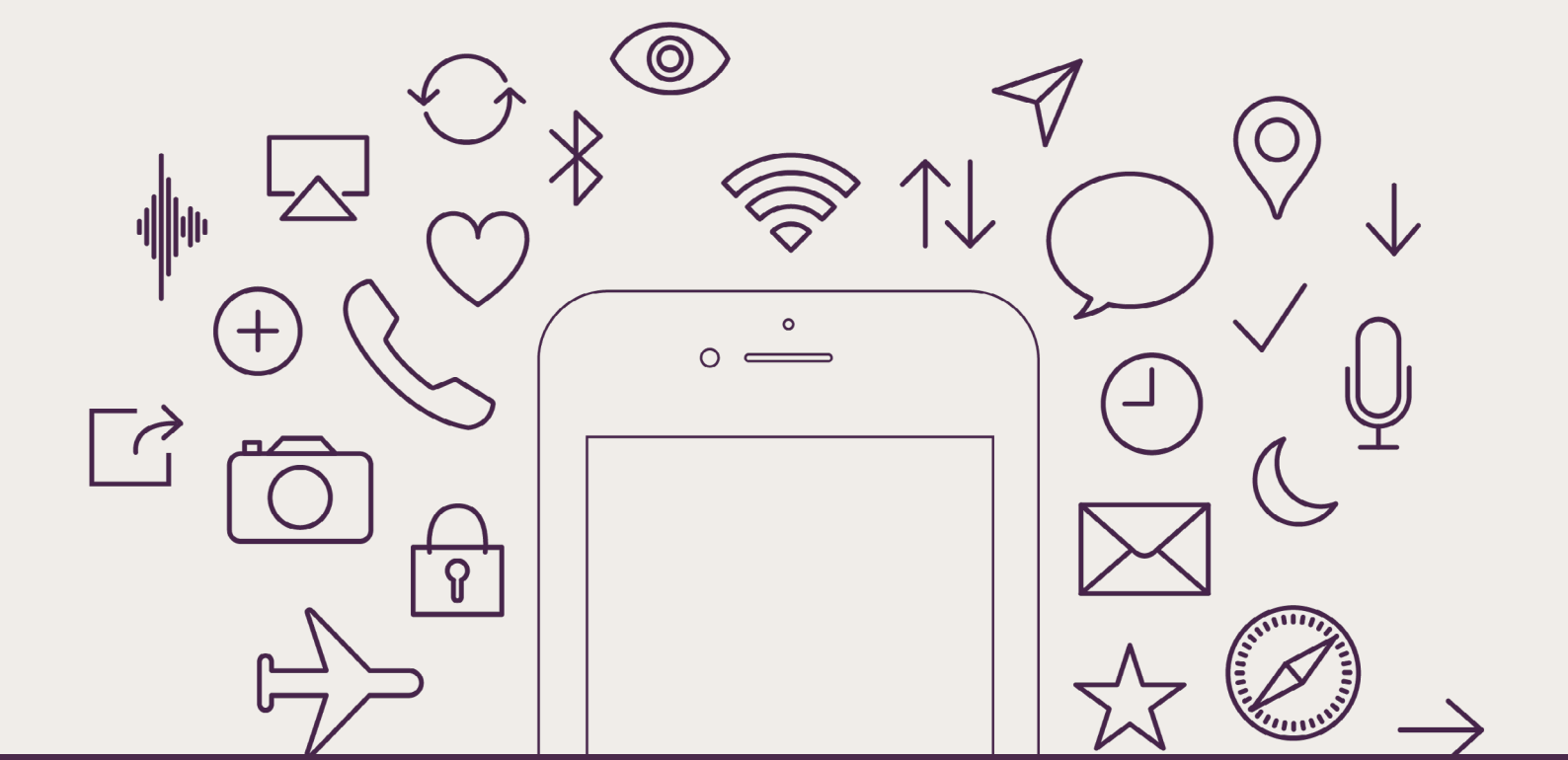


GUIA PRÁTICA DE ESTRATÉGIAS E TÁTICAS PARA A SEGURANÇA DIGITAL FEMINISTA

CFEMEA

Titulo: Guia Prática de Estratégias e Táticas para a Segurança Digital Feminista

CFEMEA - Centro Feminista de Estudos e Assessoria
SCS, Quadra 2, Bloco C, Ed. Goiás, Sala 602
70317-900 - Brasília, DF, Brasil
Telefones: (61) 3224-1791
www.cfemea.org.br

Coordenação geral: Jelena Dordevic e Fernanda Shirakawa

Textos: Fernanda Shirakawa, Fernanda Monteiro e Larissa Santiago

Revisão e edição: Cristina Lima

Contribuições: Priscilla Britto, Joana Varon e Carla Jancz (revisão)

Projeto gráfico e visual: Maria Rita Casagrande

Tiragem: eletrônica

Realização: Centro Feminista de Estudos e Assessoria – CFEMEA e Universidade Livre Feminista, em parceria com Blogueiras Negras e Marialab.

Apoio: Oak Foundation e Ford Foundation

Universidade Livre Feminista
Ação colaborativa compartilhada por Centro Feminista de Estudos e Assessoria – CFEMEA, Cunhã Coletivo Feminista e SOS Corpo – Instituto Feminista para a Democracia.

www.feminismo.org.br

GUIA PRÁTICA DE **ESTRATÉGIAS E TÁTICAS** PARA A **SEGURANÇA DIGITAL FEMINISTA**

Nossos corpos,
Nossa resistência na internet

maria [lab]

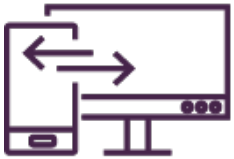
BLOGUEIRAS NEGRAS

Universidade Livre Feminista

CFEMEA

SUMÁRIO

INTERNET:
por mais segurança para nós, mulheres.



Esta Guia Prática de **Estratégias e Táticas** para a **Segurança Digital Feminista** tem o objetivo de proporcionar às mulheres maior autonomia e segurança na internet, apresentando estratégias e táticas de defesa digital para feministas. Os conteúdos são dirigidos para o público de mulheres da América Latina e foram elaborados considerando diferentes mulheres: negras, trans, lésbicas, ativistas/militantes de movimentos organizados de mulheres ou que atuam individualmente na rede, sendo de periferias urbanas, rurais, com distintos níveis de acesso à tecnologia nas suas abordagens.

Cada assunto está conectado com casos reais de violência *on-line* e possui informações práticas de como agir para enfrentarmos as adversidades em cenários semelhantes. Primeiramente, apresentamos o que é e como identificar o mosaico de ameaças e como traçar um percurso para a defesa digital, analisar riscos e entender onde focar os esforços quanto à segurança.

A segunda parte do conteúdo será dedicada ao uso de celulares para nossas comunicações, em como ter um aparelho mais seguro e poderoso contra a violência institucional, de onde quer que ela venha.

Abordaremos também o que fazer nas redes sociais para combater discursos de ódio, "**vingança pornô**[1]" , por exemplo, e derrubada de páginas. E também explicaremos como configurar perfis de forma segura e fazer denúncias sem correr o risco de exposições.

[1] A pornografia de vingança é uma modalidade que comumente expõe vídeos íntimos de mulheres, geralmente por seus ex-parceiros (ou parceiras), com a intenção de constrangê-las e assediá-las, como se fossem culpadas pela sua sexualidade. Estes vídeos também podem se tornar objetos de chantagem financeira e emocional, inclusive podendo causar transtornos profissionais e familiares na vida destas mulheres, resultado da visão patriarcal e misógina que ainda persiste em nossa sociedade sobre o sexo.

O último bloco de conteúdo da Guia irá explicar como podemos manter nossas contas, comunicações e arquivos digitais mais seguros, explicando como usar criptografia de arquivos, manter senhas seguras, o que fazer para se proteger em conexões públicas e *lan-houses*.

Esperamos que a leitura seja útil para a sua vida digital e ajude nossa revolução digital feminista acontecer.

> *Feministas perturbam sistemas, espaços e eventos que oprimem, violam e nos impedem de viver livremente, de expressar nossos desejos e de criar vidas alternativas, seguras e realizadas. A internet é um espaço, uma plataforma, um conector digital que usamos cada vez mais para agitar, comunicar e mobilizar. Enquanto a vigilância estatal de ativistas aumenta,* ***trolls*** *misóginos geram violência, empresas coletam as nossas informações e invadem a nossa privacidade.*
> *Precisamos perturbar e contestar a Internet! Através de ativismo coletivo, movimentos interligados e compreensão da natureza e da governança da Internet, feministas iniciaram uma perturbação coletiva ao imaginar uma Internet Feminista[2].*

Fonte: Imagine uma internet feminista

[2] Disponível em: http://www.forum.awid.org/forum16/pt-br/posts/recodificando-o-poder-hackeando-ocupando-e-criando-uma-internet-feminista. Acesso em: 18 set. 2017.

INTRODUÇÃO

Nos últimos anos, o movimento feminista vem ocupando de diversas maneiras o espaço da internet, em especial das redes sociais. Mais do que usá-las como ferramentas de difusão de ideias, as feministas têm se apropriado delas como forma de encontro, discussão, mobilização, organização e articulação, promovendo uma verdadeira transformação nos modos de existir do próprio movimento e da sua relação com a sociedade. Para citar exemplos, foi possível colaborar em processos importantes da política nacional, visibilizando lutas feministas e do movimento de mulheres negras, como a Primavera das Mulheres e a Marcha das Mulheres Negras, respectivamente. No entanto, as ativistas e os coletivos feministas que se destacam pela sua atuação nos espaços virtuais também passaram a sofrer com a vigilância e com as mais diversas manifestações de violência, numa reação das forças conservadoras e misóginas que também vêm se fortalecendo e ganhando adesão na rede.

A crescente criminalização de movimentos sociais, organizações, coletivos e ativistas que atuam na defesa dos direitos humanos no Brasil se intensificou a partir de junho de 2013 e particularmente desde o golpe institucional que destituiu Dilma Rousseff da Presidência da República[3]. Esse processo tem sido facilitado e legitimado pela vigilância nos meios digitais e pelas leis resultantes das tentativas de controle das manifestações provocadas por uma diversidade de fatos, mas principalmente pelos grandes eventos esportivos dos últimos anos no país.

[3] O instrumento da Garantia da Lei e da Ordem (GLO) e a Lei 12.850/2013 (Organizações Criminosas) estão sendo usados para justificar infiltrados e perseguições em redes sociais. Não faz muito tempo que a mídia repercutiu casos como o de Elisa Quadros e Balta Nunes, histórias em que o abuso de autoridade e o uso intencional de violências psicológicas são agravados quando as vítimas são mulheres.

A atual conjuntura política de crescente restrição de direitos e de fortalecimento de segmentos ultraconservadores favoreceu que a Câmara dos Deputados se mobilizasse em torno de inquéritos como a CPI do Aborto, intensificando a criminalização sobre o direito reprodutivo das mulheres e as organizações e movimentos que pautam esta luta no Brasil.

Segundo o *Dossiê Criminalização das mulheres pela prática do aborto (2007-2014)*, citando uma pesquisa realizada pelo Instituto de Estudos da Religião, no Rio de Janeiro, das mulheres que tiveram ocorrências registradas por aborto, um total de 55% são não-brancas. Este mesmo Dossiê aponta a criminalização das organizações nacionais e internacionais que foram citadas na CPI do Aborto, com o objetivo de – segundo os deputados - "investigar a existência de interesses e financiamentos internacionais para promover a legalização do aborto no Brasil (...) contra a vontade do povo e do Congresso".

Não obstante, nós, mulheres, atuando em movimentos organizados ou mesmo como ativistas que atuam individualmente na rede, estamos sujeitas a essa vigilância e à violência que ameaçam o direito aos nossos corpos e vidas.

Por conta dessa ofensiva conservadora, nos tornamos vulneráveis aos mais diversos tipos de violências nos espaços que ocupamos ou pelos quais transitamos cotidianamente. Nas ruas, casas, ambientes de trabalho, movimentos, nossos corpos são alvo constante do assédio, do estupro, do racismo, da lesbofobia e da transfobia. Somos julgadas pela nossa aparência e comportamento. E se, nos espaços públicos, travamos uma batalha em defesa de nossos corpos e nossos direitos, o mesmo acontece nos virtuais. No caso de novos espaços públicos, como a internet, onde nós, mulheres, nos apropriamos dessas discussões? A que tipo de violências estamos sujeitas? A violência nas ruas, nos espaços físicos, tem reflexo no espaço virtual?

No entanto, apesar da gradual ocupação desse espaço pelas organizações feministas e por feministas atuando de forma individualizada, ainda discutimos pouco a que violências estamos sujeitas na internet. Seriam as mesmas que vivemos *off-line*? Ou têm características específicas?

> [...] parecida com a violência nas ruas, a violência na internet supõe um ataque altamente sexualizado, onde os corpos das mulheres são o foco do ataque e que inclusive enfrentam as ameaças de ataques sexuais concretos. (Análise Feminista de Políticas da Internet 2016, GenderIT.org[4]).

Como podemos nos proteger da violência no espaço virtual?

Os anos de luta dos movimentos feministas e de mulheres contribuíram para dar visibilidade a questões sobre violência e levaram à conquista de importantes mecanismos de proteção e apoio, como os previstos pela Lei Maria da Penha. Mas, e na internet? Que mecanismos deveriam nos garantir maior proteção e apoio?

O Marco Civil da Internet[5] estabelece, no seu 11° artigo: "[...] deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das

[4] Disponível em: https://www.genderit.org/es/feminist-talk/principios-feministas-para-internet-segunda-versi-n. Acesso em: 19 out. 2017).

[5] Lei de iniciativa e participação popular sancionada em 2014, que reflete uma árdua luta do movimento pela democratização da comunicação no Brasil. Prevê algumas mudanças quanto ao uso da internet no país, garantindo direitos, estabelecendo princípios e deveres, como o que diz respeito à privacidade.

comunicações privadas e dos registros". Assim, esta lei deveria nos proteger, como pessoas que acessam a rede, de termos nossos dados e comunicações interceptadas por empresas ou quaisquer outros órgãos. Mas, na realidade, o que temos, inclusive, é uma ameaça a nós através do ataque ao próprio Marco Civil da Internet, com deputados e senadores pleiteando mudanças que ferem seus princípios (como o da **neutralidade da rede**) na tentativa de tirar a seriedade da lei.

Ao contrário, temos exemplos de diversos mulheres que são ameaçadas constantemente por ex-namorados, companheiros, chefes e outros homens em casos de vingança pornô, onde fotos, dados e outras informações são expostas, levando a violência *online* a extremas consequências na vida real.

Ao mesmo tempo, o movimento feminista organizado e coletivos feministas têm suas páginas, blogs e outros canais na rede frequentemente invadidos por h*ackers* e grupos que querem minar nosso diálogo com a sociedade. As ameaças também partem dos governos, dos aparelhos repressores do Estado e de camadas conservadoras da sociedade, quando atacam as mulheres em suas produções de conteúdo (fotos ou textos), expondo imagens e informações e principalmente quando as ameaçam no intuito de atacar sua integridade física.

Como então construir e participar de maneira segura de espaços *online*, que estão sendo constantemente ameaçados e que se tornam inseguros para as mulheres? O que devemos conhecer, entender e como reagir a ataques, ameaças e violências online que ultrapassam a barreira virtual?

A partir dessas questões, nós das Blogueiras Negras, do CFEMEA, do Marialab e da Universidade Livre Feminista, a partir de uma primeira discussão no 13° Fórum Internacional Awid, realizado na Bahia, em 2016, iniciamos um processo de mapeamento de casos de ataques a ativistas em meios digitais e de discussão de estratégias que grupos feministas e de mulheres vêm formulando para enfrentar a cultura de ódio que se espalha pela internet. E propusemos o desafio de pensar o enfrentamento das violências que acontecem principalmente *on-line*.

Embora no *off-line* estejamos mais acostumadas a pensar em soluções coletivas para a nossa organização e segurança, usamos as redes sociais sem nos atentarmos para os riscos a que estamos sujeitas. A luta e a resistência na internet parecem ser profundamente individualizadas, o que torna determinadas ativistas alvos fáceis de ataques.

Outra reflexão importante é como usarmos esse espaço de uma forma anticapitalista, que questione a hegemonia dos "donos" da internet, em sua maioria homens brancos, cis e heterossexuais. Estes latifundiários das ideias controlam um volume inimaginável de informações sobre nós, que são vendidas às corporações mais questionadas e enfrentadas pelo movimento feminista, como a indústria farmacêutica, por exemplo.

Para tentar avançar nessas reflexões, nós lançamos uma iniciativa conjunta que consiste em um mapeamento das violências sofridas por feministas e mulheres ativistas no âmbito da internet; e na formulação de materiais e conteúdos sobre segurança digital; além de atividades de debate e reflexão sobre como montar estratégias coletivas para lidar com essa questão.

> *Uma internet feminista trabalha desenvolvendo mais empoderamento para mulheres e pessoas* queer *– em toda a sua diversidade – a fim de fazer-nos participar inteiramente dos nossos direitos, nos engajando no desejo e num modo de desmantelar o patriarcado; isso leva em consideração nossas diferentes realidades, contextos e especificidades – incluindo idade, deficiências, sexualidades, identidades de gênero e expressões, lugares na pirâmide socioeconômica, crenças políticas e religiosas, origens étnicas e marcadores raciais.*

Guia Princípios Feministas da Internet, APAC, 2016.

Violência
na internet.

Como um lugar onde expressamos nossas ideias, compartilhamos sentimentos e ações, a internet também é um lugar permeado por violências. Entendendo que as fronteiras entre o *on-line* e o *off-line* não são rígidas, e que vivemos em um mundo onde o virtual cada vez mais faz parte da nossa experiência concreta, o racismo, o machismo, a lesbofobia, a transfobia, dentre outras opressões, têm equivalências nos dois espaços.

Embora tenha dinâmicas de interação específicas, a internet é repleta de disputas de poder, discursos de ódio, expressões de amor e outras tantas iniciativas. Sua potencialidade em viralizar conteúdos, na verdade, tem sido uma forma de espalhar o ódio na velocidade típica da rede e faz com que os efeitos sofridos (sentidos) sejam longos, doloridos e, por vezes, fatais. Apresentamos aqui alguns casos recentes vividos por mulheres que foram atacadas ou sofreram diferentes tipos de violência, mas todas com uma característica comum: são ativistas, do movimento de defensoras dos direitos humanos, feministas ou não. Todas elas lutando dentro da rede, e fora dela, por uma sociedade mais justa e igualitária.

1) JÉSSICA IPÓLITO

Um dia Jéssica resolveu postar uma foto sua no *Facebook* junto com um texto falando da autoestima como mulher negra, gorda e lésbica, incentivando as mulheres a amarem seus corpos. Em menos de 24horas, seu *post* tinha milhares de comentários [quatro mil, pra sermos mais específicas], onde homens a xingavam e agrediam com discursos carregados de racismo e gordofobia. Um ataque em massa de homens que participam de fóruns de direita, de fóruns racistas – identificados pela própria Jéssica. Algumas mulheres haviam feito comentários positivos, mas isto não inibiu a ação dos racistas e gordofóbicos. Depois do grande número de denúncias realizadas em uma foto de Jéssica, denúncia essa realizada em massa, o *Facebook* desativou sua conta por quatro dias – ou seja, vítima de racismo e gordofobia, ela ainda ficou sem poder publicar ou interagir na sua própria conta. A política de privacidade daquela plataforma permite que ataques como esse sejam realizados e que as pessoas que são vítimas desses criminosos ainda sejam punidas.

Como desfecho, Jéssica resolveu denunciar as pessoas que fizeram os comentários racistas e paralelamente, mulheres feministas na internet escreveram manifestos, textos de apoio e palavras de solidariedade para Jéssica.

2) MARIA RITA CASAGRANDE

Maria Rita está na internet há muito tempo. Para sermos mais exatas, desde 1997, escrevendo no seu primeiro blog – *O Império dos Sentidos* –, onde seus relatos pessoais podiam ser lidos e comentados. Desde então, ela nunca mais parou. Um dos seus blogs mais conhecidos e mais acessados é o *True Love - Cultura Lésbica e Bissexual*, onde escreve sobre relações, amor, corpo e política. E justamente por estar lidando com estes assuntos de maneira tão brilhante, cutucando a ferida de empresas e instituições e sobretudo por tratar de questões sobre sexualidade e corpo, Maria Rita foi atacada inúmeras vezes. Sua caixa de comentários sempre esteve cheia de ameaças, xingamentos, racismo, expressões de gordofobia e agressões. No caso de Maria Rita, os criminosos chegaram a pegar seu número de telefone para ameaçá-la. Outra vez, enviaram-lhe cartas pelo correio e e-mails com a foto de seu filho brincando no portão de casa, obrigando-a a mudar de endereço.

A violência *on-line* trouxe consequências reais: imagine você precisar se proteger, mudar de telefone, endereço, criar outros perfis nas redes sociais e ter sua família e integridade física ameaçadas? A militância *on-line* de Maria Rita Casagrande incomodou os racistas e machistas de plantão, mas ela não desistiu e continua a escrever e denunciar.

3) JAQUELINE
GOMES DE JESUS

Jaqueline Gomes é doutoranda em psicologia social e militante transfeminista. Ela tem atuado tanto *on* quanto *off-line*, no que diz respeito às questões de identidade de gênero e raça, interseccionando as lutas. Recentemente, Jaqueline usou seu *twitter* para falar sobre a vitória de Trump nas eleições dos Estados Unidos da América, o que isto significava para países como o Brasil, por exemplo. Segundos depois, homens que se consideram "a direita no Brasil" começaram a responder seu *tweet* com violência, acusando-a de comedora de mortadela, afirmando que a esquerda está apanhando desde 1964 (utilizando imagens de policiais batendo em pessoas) e mandando Jaqueline mudar o seu sobrenome, alegando que, se ela falava de fundamentalismo religioso, seu nome não deveria ter "Jesus".

Os insultos e xingamentos continuaram, apesar de Jaqueline não responder a nenhum, apenas compartilhando os *prints* no seu próprio *Facebook*.

Cada vez mais, transfóbicos, racistas e misóginos se sentiram à vontade para silenciar as mulheres, impondo suas opiniões de forma violenta e destilando discursos de ódio *on-line*, o que, já sabemos, traz consequências reais; legitimando atitudes racistas, violência física e agressões como as sofridas por militantes da esquerda que trajavam vermelho nas eleições brasileiras em 2014.

A Guia

Apesar de todo esse cenário de violências *on-line* que se expande, pouco se faz de fato para tornar esse território digital um ambiente livre de misoginia, transfobia e racismo. As agressões são inúmeras e sistemáticas, e tendem a ser banalizadas e pouco visibilizadas e reconhecidas. Evidenciar essas violências e entender como nos defender talvez sejam os primeiros passos para criar um ambiente digital mais seguro.

Mas como reagir em um meio onde nos sentimos muitas vezes sozinhas e inaptas?
O que muita vezes não nos damos conta é de que nós, mulheres, somos a maioria do público da internet brasileira, totalizando 54,7% (IBGE) dos acessos em 2014. Apesar de muitas de nós – como mulheres negras, pobres e periféricas – não termos o devido acesso, constituímos uma parcela significante das que consomem notícias e criam conteúdo. E se a internet é formada pela rede de pessoas que a acessam, nós de fato somos parte dessa rede e podemos construir resistências, articular defesas e lutar pela sua reapropriação feminista, mesmo com nossas limitações e percalços de acesso às tecnologias.

Por que
uma Guia?

Na América Latina inteira, temos vivido constantes ataques à democracia que implicam a redução ou completa retirada dos nossos direitos. Países como Honduras, Paraguai, Argentina e Venezuela têm passado por complexos processos de golpes, onde governos ilegítimos têm cortado investimentos, sucateado educação e saúde e sobretudo atacado ativistas dentro e fora da rede.

Recentemente a Venezuela protagonizou um desses casos: alguns canais de TV pela *web* tiveram suas transmissões cortadas devido a uma "falha de conexão" apenas com usuários que usavam **VPN**[6] para se conectar. Ciberativistas mencionaram o bloqueio de **DNS**[7] de alguns canais e da própria provedora de internet, a VivoPlay. A violência migrou da rede e foi pras ruas quando policiais agrediram e prenderam um cinegrafista da televisão local enquanto ele cobria os protestos em Caracas.

No Brasil, desde 2013, as leis que criminalizam ativistas dos movimentos sociais em geral têm ganhado mais aliados no discurso e na prática. Não só políticos e instituições do Estado, como a polícia, têm trabalhado para impedir protestos e organizações, como os/as próprios/as cidadãos/ãs têm absorvido o discurso de que estar na rua ou na rede lutando por direitos é coisa de "vândalo". Como mulheres, temos sofrido o retrocesso de forma mais intensa, já que nossas demandas como feministas, mulheres negras, trans e de movimentos urbanos e rurais têm sido abafadas não só pelo silenciamento cotidiano, mas principalmente pela cultura da intolerância, demonização e criminalização dos movimentos. Assuntos como aborto, direitos reprodutivos e sexuais, gênero e raça são sempre tabus que geram agressões gratuitas, discursos de ódio e incitação a violências que tomam proporções gigantes, como as que veremos nesta Guia.

Reconhecemos que estamos sofrendo violências *on-line* sistemáticas e que não temos muitas guias específicas para feministas, principalmente voltadas para as mulheres da **América Latina**, que têm características de raça, classe social e identidades diferentes.

---

[6] *Virtual Private Network*: uma conexão de acesso privado e parcialmente anônima, onde você conecta a um servidor que permite a você utilizar outra rede através dele, escondendo assim o seu endereço IP e metadados de navegação do resto da rede.

[7] *Domain Name System*: sistema que permite que um servidor tenha um nome único reconhecido por toda a internet, gerenciando e direcionando o acesso feito aos endereços de internet.

Como analisar
o cenário de vigilância?

Antes de começar com sua leitura, é importante entender que essa Guia não está aqui para adicionar mais paranoia a sua vida, mas para apresentar estratégias e táticas para defesa de ataques machistas nos meios digitais. Leve em consideração seu uso e frequência na rede, sua prática com tecnologia e aparelhos (se tem ou não *smartphone*) e, sobretudo, os lugares de onde você acessa. Não há motivos para pânico, o nosso desejo é conversar e informar!

Para percorrer nossa Guia, aconselhamos uma análise sobre o mosaico de ameaças que faz parte da nossa vida, pois cada uma de nós tem forças e fraquezas diferentes, assim como vivemos contextos culturais e sociais diversos, e entender quais estratégias são fundamentais para nossa segurança digital é o primeiro passo. Por **mosaico de ameaças**, chamamos os principais cenários que podem nos deixar mais vulneráveis. Definir estes cenários nos ajudará a focar nossas energias no que é mais urgente e sensível para nossa segurança.

MOSAICO DE AMEAÇAS

Como identificar
onde começo?

Somos pessoas diferentes, estamos em contextos diferentes e as possibilidades de estarmos em uma situação de perigo, seja *on-line* ou não, são múltiplas. Por isto, antes de entrar na paranoia, sabendo de todas as possíveis vulnerabilidades que enfrentamos na nossa vida, é essencial analisarmos as ameaças que são específicas do nosso contexto.

Entendemos por ameaça tudo aquilo que é externo a nós e que pode nos causar um dano. As ameaças podem ser virtuais ou não e estão presentes na nossa vida o tempo todo. Para ilustrar esta definição, vamos falar de uma coisa simples, como um dia de chuva na vida de duas pessoas diferentes: Ana e Isabel. Ana deve sair de casa e percebe que pode chover e esfriar, e analisa a possibilidade de se molhar e passar frio como uma ameaça a sua saúde, e para se precaver leva um casaco e guarda-chuva. Isso é muito importante para Ana porque geralmente fica resfriada nessas situações.

Já Isabel não acha que o fato dela se molhar seja uma ameaça tão grande, pois mora numa cidade muito quente e dificilmente fica doente. Então mesmo que esfrie um pouco, ela sabe que nada vai

acontecer com sua saúde. Porém pode ser que Isabel tenha mais possibilidades ser picada pelo mosquito que transmite a Zica e então levar repelente ao sair de casa seja muito mais essencial para ela que se lembrar de pegar o guarda-chuva, como Ana.

Aqui as duas analisaram as suas ameaças e escolheram se assegurar daquela que parecia mais grave. Como os contextos das mulheres são muito diferentes e formados por diversas características externas e internas como aspectos geográficos, culturais, sociais, econômicos, psicológicos, físicos e digitais, entendemos essa combinação como um mosaico de fatores que influenciam a nossa análise das ameaças. Por isto estamos usando esse termo para entender o contexto e o que fazer para nos proteger.

Uma forma simplificada de fazer isto é analisar o que se quer assegurar e de quem se quer proteger. Por exemplo, pode ser uma comunicadora pode querer proteger suas informações pessoais de possíveis agressores machistas, ou ser uma defensora de direitos humanos e querer proteger seus contatos de empresas e governos que têm interesses em impedir suas ações de protesto.

Percebemos que para cada pessoa existe o que chamamos de Mosaico de Ameaças, e entendê-lo é o primeiro passo para saber onde focar as suas prioridades em relação a sua segurança digital.

Antes de começar essa leitura tente fazer este exercício, refletindo sobre:

O QUE VOCÊ ESTÁ TENTANDO PROTEGER?

DE QUEM VOCÊ ESTÁ SE PROTEGENDO?

Abaixo listamos algumas dessas respostas em “O que vou proteger?” e “De quem vou proteger?” para nos ajudarem a achar as estratégias e táticas que servem a algumas ameaças. Contudo é importante lembrar que as respostas listadas aqui são apenas exemplos. Você poderá encontrar **outras razões para se proteger de algum outro risco**, e dessa forma desenhar sua estratégia e suas táticas mais adequadas.

Não esperamos dar respostas prontas para nossos problemas, mas desejamos que os conteúdos dessa Guia provoquem o pensamento em relação à segurança digital. Segurança é uma mudança de comportamento, e não um aplicativo ou programa instalado no computador ou celular.
Boa leitura! ;)

Celular

CASO 1

Estava a caminho da minha casa, quase chegando na comunidade de moto quando fui abordada por policiais encapuzados que, ao me revistarem ilegalmente, tomaram meu celular e olharam minhas fotos, mensagens, agenda. Tive medo deles vendo minhas informações no celular, mas tive mais medo ainda do que eles poderiam fazer comigo na abordagem e ao descobrirem que sou ativista e lésbica.

Estratégia 1

Tenha um celular mais seguro em caso de apreensão, perdas ou roubos.

O que vou proteger: contatos telefônicos, arquivos que estão no celular (texto, áudio, fotos e vídeos), mensagens de *chat*.

De quem vou proteger: qualquer pessoa que roubar ou tiver acesso ao meu telefone, adversários políticos interessados nas minhas informações pessoais, opressores etc.

TÁTICAS DE DEFESA 1 :

O que fazer imediatamente:

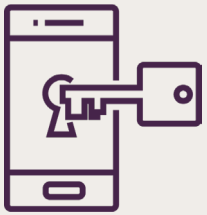
1) Bloqueie o seu chip: Ligue para sua operadora e peça para bloquear o seu chip. Essa é a única forma de desconectar algumas das suas contas e aplicativos, como o *WhatsApp*.

2) Desconecte e apague os arquivos que estão no seu celular remotamente:

Para *Androids*, acesse: https://www.google.com/android/devicemanager
Para *Iphones*, acesse: https://support.apple.com/pt-br/HT201472

3) Procure ficar calma! Para o caso de uma abordagem policial ilegal, tente relaxar e respirar fundo, fale pouco e só responda o necessário. Caso seu celular não seja "baculejado" (apreendido), tente discretamente entrar em contato com alguém de sua confiança, avisando para onde você está sendo levada, se for este o caso.

O que fazer antes para não ter problemas depois:



1. Como configurar os acessos ao meu celular?
2. Arquivos escondidos: como esconder aquelas fotos que só você quer ver?
3. Criptografe tudinhoooo
4. Como reduzir o dano em caso de perda do conteúdo do celular?
5. Alguém pode me obrigar a revelar a senha do celular?
6. Meu telefone celular é bem antigo, só faz chamadas e sms. O que posso fazer?

1. Como configurar meu celular?

Você tem senha no seu celular? Se não tem, presta atenção na dica!

Ter uma senha no celular é fundamental para não deixar tão fácil a vida de quem quer bisbilhotar suas informações. E isto não quer dizer que seja somente no caso de ter o celular apreendido, roubado ou perdido, mas também quando você deixar o celular dando bobeira para uma pessoa com interesse no seu ativismo instalar **programas espiões** no seu celular. Afinal, vamos falar a verdade, nosso celular virou nosso diário interativo e nosso meio de nos comunicarmos com todas as pessoas da nossa vida.

Então vamos lá. Se você não configurou ainda sua senha, aqui vão as dicas. Caso já tenha feito isto vá para o **item 2** deste bloco.

Para configurar sua senha no *Android,* acesse **Configurações > Segurança > Tela de Bloqueio**. Entre as opções, escolha **Senha (palavra frase)** e escreva sua senha nova.

#FICAADICA: escolha uma palavra fácil de lembrar e anote em um papel até não esquecê-la mais. Depois descarte o papel de forma segura (rasgando ou queimando).

A opção de uma palavra é muito mais segura que o **Deslize** ou que o **PIN de números**, pois estes têm poucas opções de combinações e podem ser visualizados através da gordura dos dedos na tela (tente fazer o teste no seu celular inclinando a tela e percebendo que a marcação da senha se revela), sendo assim são fáceis de adivinhar.

Para *Iphone,* ainda existe a opção de dar a sua **Digital** ou **Reconhecimento Facial**[8] como forma de acesso, mas não recomendamos nenhuma dessas duas formas, pois apesar de parecerem fáceis e simples, elas aumentam o acúmulo de informações pessoais sobre sua identificação por terceiros, como é o caso da empresa *Apple*.

Além disso esses modos podem ser inseguros pois se apoiam em uma função do celular que pode "bugar" (dar problema) a qualquer momento.

Para alterar a senha no *Iphone* acesse **Ajustes > Código > Alterar Código > Escolher Passphrase ou Senha de caracteres Alfanuméricos.**

Para ***Windows Phone*,** ir em **Configurações > Bloqueio > Alterar a senha.**

[8]Técnica de **biometria** baseada nos traços do rosto das pessoas. A técnica feita através de computadores define traços únicos que devem ser mapeados em códigos, reconhecendo pessoas dos mais variados biotipos.

2. Arquivos escondidos:
como esconder aquelas fotos que só você quer ver?

Esconder arquivos no celular usando alguns aplicativos vai garantir maior privacidade para a suas fotos, vídeos e contatos que estão armazenadas dentro do aparelho. Numa situação de apreensão ou abordagem como a do exemplo, o risco de você ter suas informações reveladas pode reduzir a zero. Pense nisto!

Aqui vamos dar dicas de aplicativos que permitem que você possa colocar esses arquivos em uma pasta secreta a que só você tem acesso. Assim você assegura maior segurança em esconder fotos arquivos e, se alguém tiver acesso ao seu celular, será mais difícil vasculhar sua vida. Além disso você terá maior discrição na hora de acessar o álbum de fotos, pois você pode esconder todos seus ***nudes*** em outra pasta e não arriscar revelar aquela foto *bapho* para a família quando estiver mostrando as fotos das férias passadas, por exemplo.

Esses aplicativos são:

Para *Android*, o ***Secrecy***: é um aplicativo de código aberto disponível para *Android* que usa um sistema de **criptografia** conhecido e testado. Ele é fácil de instalar e é gratuito.

Quando se instala o aplicativo, ele nos redireciona para uma página de apresentação do *app* (em inglês). Depois de visualizar a página de explicação, abra o aplicativo e clique no símbolo "+" e adicione um novo cofre. Nomeie o cofre como preferir e crie uma senha boa, mas que você possa lembrar (importantíssimo!!). Depois de criar o cofre, clique no nome dele e coloque sua senha. Isto abrirá o cofre, e lá dentro você poderá adicionar as imagens que quiser clicando no símbolo "+". É importante perceber que - uma vez adicionadas dentro do cofre - as imagens não aparecerão mais

na sua Galeria de Fotos e só poderão ser vistas ou acessadas para compartilhar dentro do cofre. Por isto, minas, "não se esqueçam da senha!!".

O legal desse aplicativo é que ele criptografa seus cofres e fica quase impossível uma pessoa acessá-lo sem sua senha. Muito importante para nossos segredos.

Existem muitas outras opções de aplicativos similares ao *Secrecy*, como o ***Cofre KeepSafe***. Mas eles não são de **código aberto**, o que não nos deixa entender se o que prometem fazer é realmente verdade, mas para quem tiver dificuldades com o *Secrecy*, vale a pena dar uma olhada nas outras opções, ficando atenta para as permissões que o *app* pede e para as avaliações na loja de aplicativos do *Google*, a *PlayStore*.

Para *Iphone,* tente o ***Securepad*** e, para *Windows Phone* o ***Pic Lock Ultimate***.

3. Criptografe tudinhoooo.

Então, vamos lá! Por que depois de colocar a senha para acesso você ainda teria que se preocupar com outros tipos de proteções?

Bom, o mundo não é tão fácil assim, como todas sabemos ;) e infelizmente, mesmo com uma boa senha ainda é possível que alguém consiga acessar suas informações no celular caso ele seja apreendido, roubado ou perdido.

Isto porque, conectando seu celular num computador, é possível acessar os arquivos dentro da memória do telefone mesmo sem ter a senha de acesso. E além disso, mesmo fazendo um "*Factory*

reset" ou "Restaurar configurações de fábrica", sombras dos arquivos apagados ainda ficam na memória do celular e é possível recuperar fotos, vídeos e outros dados.

Por isto, recomendamos que, se você tiver *Android* a partir da versão 4.1 (**veja aqui como checar a versão do celular**), criptografe o celular integralmente.

Antes de seguir com o procedimento, é recomendável fazer um ***backup* dos seus arquivos** (veja o próximo item 4).

Para criptografar seu celular, vá em **Configurações > Segurança > Criptografar telefone** *(em algumas versões aparece como Codificar - não se espanta, é a mesma coisa)*. O telefone irá precisar da bateria do celular cheia e um pouco de tempo para que seu telefone faça o procedimento (máximo 30 minutos).

Para encriptar *Iphone,* **veja essas dicas**:

O *Windows Phone* permite a criptografia na versão 10 do **sistema operacional**. Para saber mais **acesse aqui**.

4. Como reduzir o dano em caso de perda do conteúdo do celular?

Importante fazer o *backup* de tudo!!

O *backup* nada mais é do que uma cópia de segurança dos seus arquivos em outro local, por

exemplo, manter suas fotos e contatos do celular no seu computador, ou seus documentos do computador em um **HD** externo ou em um serviço de armazenamento na nuvem. Lembrando que é sempre bom fazer isto com frequência - dependendo claro do quanto você tem de informação você tem guardada no seu celular.

O jeito mais recomendado é fazer *backup* baixando as informações do seu celular no seu computador com um cabo USB. E como fazer isto vai depender do modelo do seu celular e do aplicativo recomendado, mas geralmente conectando o seu celular o computador você irá conseguir visualizar seus arquivos.

Você também pode usar um aplicativo de *backup* ou guardar seus arquivos na nuvem, mas recomendamos ficar atenta a quais arquivos serão armazenados na nuvem. Não se esqueçam dos **casos de vazamento de nudes de celebridades** devido a cópias de arquivos no *Icloud* (nuvem).

5. Alguém pode me obrigar a revelar a senha do celular?

Legalmente, não. Se este alguém for um opressor que esteja acusando você de algo e queira saber sua senha para "averiguar" seu telefone, saiba que por Lei você não é obrigada a fornecer nada. Ao obrigar você a fornecer sua senha, essa pessoa pode quebrar um direito seu que se refere à Presunção de Inocência, garantida pelo art. 14.3, g, do Pacto Internacional sobre Direitos Civis e Políticos e no art. 8°, 2, g, da Convenção Americana sobre Direitos Humanos. Além disso, nossa constituição (art. 5°, X) garante ser inviolável a quebra da intimidade e privacidade das pessoas, e obrigar alguém a fornecer a senha é ir contra este direito.

Sendo assim, até mesmo um juiz não pode exigir a sua senha. A única coisa que o judiciário pode fazer é pedir a quebra do sigilo das suas comunicações.

Massss... sabemos que nem sempre essas coisas acontecem dentro da lei, e, às vezes, fornecer a sua senha pode ser a sua única opção numa situação de intimidação, ameaça ou coerção.

Para tentar garantir mais segurança nesses casos, recomendamos ocultar os rastros de informações sensíveis: apagando sempre as mensagens dos seus *chats*, usando aplicativos que escondem e criptografam suas informações sensíveis (item 3) e escondendo estes aplicativos através das configurações do seu telefone ou usando outros *apps* (como o ***Apex Launcher***). Caso aconteça com você alguma **situação em que seu celular seja apreendido ("baculejo")**, tente manter a calma. E procure não retrucar ou reagir, pois o que eles querem é apenas um motivo para a violência. Tente responder apenas o necessário e relaxe! Se você estiver indo em direção a sua casa ou à de alguém conhecido, após a abordagem, mude o caminho e só siga quando se sentir segura. Depois procure alguém mais próximo que seja de sua confiança e busque apoio.

6. Meu telefone celular é bem antigo, só faz chamadas e sms, o que posso fazer?

Se seu celular é mais antigo, você pode fazer algumas coisas para deixá-lo mais seguro, como habilitar uma senha para acessá-lo. Até em celulares antigos, é possível habilitar o acesso com uma senha. Para cada celular essa configuração será diferente, mas tente "fuçar" um pouco as **Configurações do seu celular**. Caso não ache nada, procure na internet. Alguém já deve ter passado por isso antes :).

Caso você tenha seus contatos salvos como "irmão", "mãe", "pai", recomendamos que você substitua pelos nomes deles ou apelidos (isto também vale pra quem tem celulares de última geração), o que pode proteger você em caso de roubo ou cópia das suas informações. Se ligue!

Outra coisa que você pode procurar fazer é uma cópia *backup* de tudo, e evitar perdas maiores, caso você perca seu celular.

CASO 2

"Eu estava na manifestação junto a um grupo de ativistas quando fui abordada por policiais e levada para a delegacia. Meus amigos foram impedidos de me acompanhar e não tinham informação para onde eu seria levada. Por conta da rapidez da ação, tive pouco tempo para contatar outras pessoas e por isso meu tempo na delegacia sozinha foi maior."

Estratégia 2

Peça ajuda de forma fácil e rápida em situações de emergência.

O que vou proteger: minha integridade física, meus direitos, caso seja presa indevidamente, para informar pessoas sobre minha localização.

De quem vou proteger: policiais que usam da força abusivamente, agressores, abusadores mal intencionados.

TÁTICAS DE DEFESA 2:

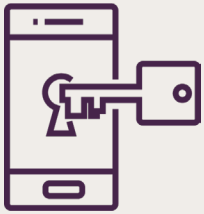
O que fazer imediatamente:

1) Tente avisar alguém que esteja perto de você no momento que está sendo abordada. Peça para esta pessoa acompanhar a abordagem enquanto ela puder. O ideal mesmo é nunca estar sozinha, mas nem sempre isto é possível.

2) Caso seu celular não seja apreendido, tente discretamente entrar em contato com alguém de sua confiança, avisando para onde você está sendo levada.

3) Se você presenciar alguém que esteja sendo detida, faça os policiais informarem para onde estão levando a pessoa e procure imediatamente o contato de algum advogado que tenha carteira da Ordem dos Advogados do Brasil (OAB). Tem uma galera dos **Advogados Ativistas, Rede Feminista de Juristas** espalhada por aí ;)

O que fazer pensando nos abusadores de plantão:



1. Existem aplicativos que podem ajudar?
2. Como posso me preparar para essas ocasiões?

1. Existem aplicativos que podem ajudar?

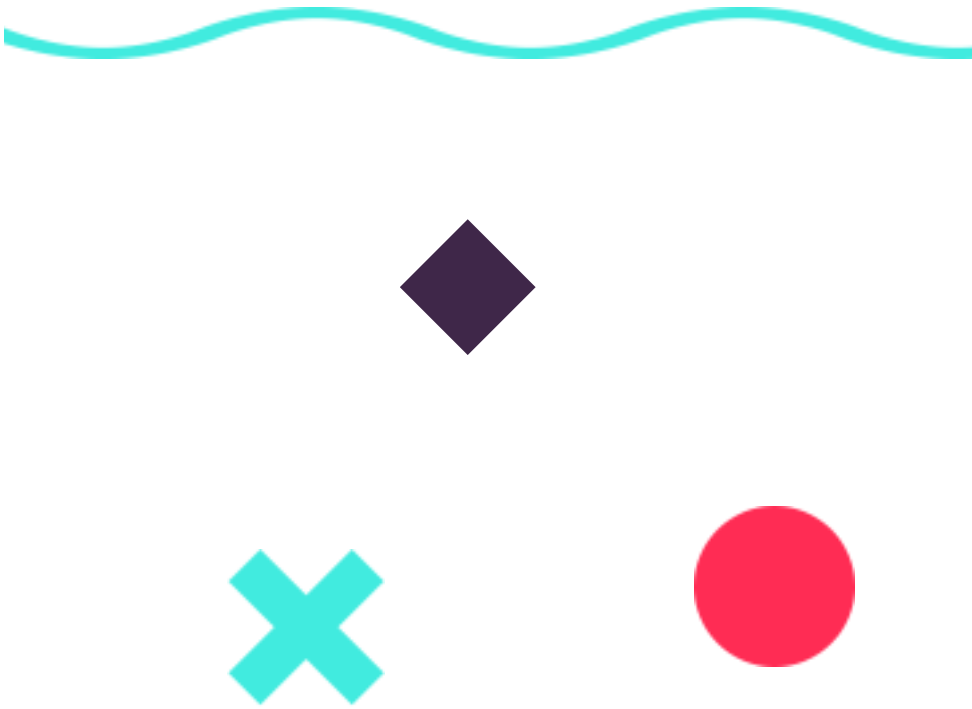
Sim, alguns aplicativos, como o **Braços Dados**, ajudam a contatar de forma rápida a sua rede de confiança. Para usá-lo, busque no seu instalador de aplicativos (*PlayStore* ou *Apple Store*) o nome desse *app* e, depois de instalá-lo, escolha os seus contatos de confiança para montar a sua rede.

2. Como posso me preparar para essas ocasiões?

Primeiro, sempre avise alguém aonde você está indo. Se você estiver acompanhada de outra companheira, deixe o número dessa pessoa com seus familiares e amigos – é importante que eles tenham como contatar você em casos extremos. Se seu celular tiver muitas informações sensíveis (conversas, contatos do seu ativismo, *nudes*, documentos privados), considere não levá-lo à manifestação, ou **apagar estas informações do seu celular**.

Caso não seja possível e o celular seja essencial para que você se sinta mais segura, lembre-se de protegê-lo (veja o caso 1), de carregar a bateria e de deixá-lo preparado para que você consiga contatar pessoas rapidamente. Isto pode ser através do aplicativo que mencionamos aqui, ou também marcando telefones como importantes para serem acessados facilmente. Você pode fazer isto adicionando números de telefones aos seus favoritos. Considere renomear alguns contatos de forma que só você reconheça quem são.

Se o seu objetivo for tirar fotos e registrar a manifestação, cheque estes dois aplicativos do *Guardian Project: Camera V* e *Obscuracam*. Eles registram (*Camera V*) ou apagam (*Obscuracam*) **metadados** com o objetivo de criar evidências ou ocultar provas, dependendo da sua intenção.



CASO 3

Na comunidade onde milito, começou a circular uma história que eu estava traindo meu marido. A traição não era verdade, mas eu estava tendo problemas no meu casamento e não entendi como pessoas estranhas sabiam de informações que não tinha falado para ninguém. Depois de algum tempo, descobri que a empresa que provocava a destruição ambiental que eu denunciava através do meu ativismo estava me monitorando pelo telefone e repassando informações para pessoas da comunidade que tinham interesse no meu cargo.

Estratégia 3

Afaste o grampo das suas ligações.

O que vou proteger: minhas conversas por telefone, minhas informações privadas.

De quem vou proteger: adversários interessados em minhas informações pessoais ou informações sobre meu ativismo.

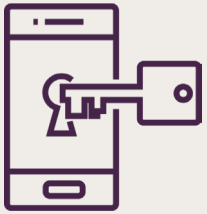
TÁTICAS DE DEFESA 3 :

O que fazer imediatamente:

1) *Como posso me comunicar?*
O grampo ainda é uma técnica de monitoramento muito usada no Brasil. Se estiver com suspeitas de estar grampeada, considere não falar coisas sensíveis ao telefone.

2) Uma das táticas pode ser marcar conversas presenciais e cafés, dependendo dos assuntos tratados. Nada melhor do que um face a face, não é?

O que fazer para se livrar do “boi na linha”[9]:



1. Entenda como funciona o grampo?
2. Por que muita gente que se preocupa com privacidade não gosta de celular?
3. O que posso fazer quando preciso falar com maior privacidade?
4. O que são metadados e por que preciso saber disso?
5. E enviar sms? É mais seguro?

1. Entenda como funciona o grampo.

Sabe aquela desconfiança de que seu telefone está grampeado porque você escuta um barulho ou porque a bateria do seu celular esquenta? A maioria dessas desconfianças são apenas paranoias. Muito dificilmente o nosso celular vai demonstrar algum efeito colateral deste tipo quando grampeado. Hoje em dia o grampo “legal” é feito direto na operadora de celular e não deixa traços. Existem, é claro, outras possibilidades, como *IMSI Catchers* e vírus diversos que podem fazer o seu telefone ficar grampeado de outras formas.

[9] Quando a presença de uma pessoa atrapalha ou intervém numa conversa ou assuntos alheios.

O grampo legal é feito através dos números IMSI (atrelado ao CPF que registrou o chip) e ao IMEI (número de fabricação do aparelho). Por isto, mudar de chip ou trocar de celular muitas vezes não é suficiente para sair do grampo.

Hoje em dia grampos são feitos em larga escala e não existe uma pessoa escutando cada conversa. Os grampos são digitais e usam programas para selecionar palavras e tom de voz das pessoas.

Alguns ***Voips***, como *Skype,* também são grampeados. Segundo os dados levantados pelo InternetLab, em abril de 2015, existiam cerca de 1.250 grampos *Voips* e 15.000 grampos de telefone por mês no Brasil.

2. Por que muita gente que se preocupa com privacidade não gosta de celular?

Os celulares de hoje em dia têm um potencial de miniaparelhos de espionagem, pois neles podemos encontrar câmera, microfone, localização geográfica (GPS) e o registro de todas as suas comunicações, além dos seus arquivos digitais como foto, áudios e vídeos. Ou seja, muita informação sobre você em tempo real.

O fato é que muitas dessas características são impossíveis de desabilitar, e portanto algumas pessoas torcem o nariz quando falamos sobre privacidade e *smartphone*, porque é verdade: os celulares não são bons com segredos.

Outra razão é que são aparelhos muito vulneráveis a serem atacados por vírus, pois muitas pessoas com más intenções desenvolvem códigos para celulares pois sabem que muita gente usando *smartphone* tem pouco controle sobre isto.

Além disso, existem vírus específicos que ganham todos os poderes do celular e são dificilmente detectados. Nos últimos anos, alguns vêm sendo usados por opressores de causas políticas, como as recentes revelações no México e no Irã.

Falando nisto, existem informações de que a Polícia Federal brasileira teve aproximação com uma empresa italiana que fabrica esse tipo de vírus, como foi revelado num vazamento de informações da **Hacking Team,** e apesar de não haver transparência quanto a **essas negociações**, pode-se deduzir que em breve esses super vírus vão tentar infectar aparelhos de pessoas no país, inclusive ativistas e pessoas dos movimentos sociais.

Por essas razões, é recomendado não deixar o telefone por perto quando estivermos falando coisas que requerem maior privacidade, pois o microfone pode estar ligado, **captando as conversas**.

Outra recomendação, principalmente para nós, mulheres, é colocar um adesivo sobre a câmera do nosso celular, pois toda precaução é pouca na hora que você sabe que seu telefone pode estar filmando você. Tem muitos tarados por aí fazendo isto. **Aqui** tem uns modelinhos ótimos de adesivos. Mas, se estiver sem grana, lembre-se que qualquer adesivo pequeno pode servir. Deixe o *glamour* para depois.

3. O que posso fazer quando preciso falar com maior privacidade?

Existem algumas opções, depende da nossa situação e de quais ferramentas temos disponíveis.

a) Se você tem um *smartphone* e consegue instalar aplicativos, tente instalar o *Signal* (mais informações no próximo capítulo) e usá-lo para fazer chamadas. Isto vai requerer que a outra pessoa com quem você vai falar também tenha instalado o *Signal* no smartphone dela.

b) Se você tem um celular com aplicativos mas não consegue instalar mais nada, tente usar o que você tem, como *WhatsApp* e *Telegram* para fazer chamadas. Estes dois aplicativos prometem encriptar chamadas de voz. O importante é ficar ligada em algumas **configurações de privacidade** e saber um pouco sobre a diferença da segurança entre esses aplicativos (veja o próximo capítulo).

c) Se seu celular não tem recursos para instalar aplicativos e nem navega na internet, considere que existe a possibilidade do grampo. Claro que isto depende de quem você é e que tipo de interesse alguém teria em realizar este tipo de espionagem. Uma solução é usar telefones públicos ou telefones não vinculados ao seu nome para ligações específicas que precisam de muita privacidade.

4. O que são metadados
e por que preciso saber disso?

Metadados são informações sobre dados digitais. Hummmmm.... Fácil, né? Só que não :) Vamos explicar melhor:

Um dado digital é qualquer coisa ou informação que você use nos meios digitais, como uma foto, uma ligação, um documento PDF, uma mensagem do *WhatsApp*, uma música, uma localização no mapa etc. Todos estes dados precisam de outras informações sobre eles para funcionarem corretamente. Por exemplo, uma foto precisa da informação do tamanho, do tipo de cores, do formato da imagem, assim como uma mensagem precisa saber para quem será enviada, quando e de onde. Todas essas informações sobre os dados, são o que chamamos metadados.

"*Ah, sim, agora que entendemos melhor o que são metadados, para que preciso saber sobre eles???*" Hoje em dia o discurso da importância da privacidade *on-line* está ganhando mais espaço, e muitas das nossas informações estão sendo criptografadas (já era a hora!).

O problema é que metadados não são muitas vezes considerados como informações sensíveis, existindo pouca regulamentação sobre o uso e acesso a eles. Mas dizem muita coisa sobre você. Por exemplo, eu posso não saber o que você falou com certa pessoa, mas eu sei sobre sua rede de contatos, com quem você fala mais frequentemente ou menos, onde você está quando você fala com essas pessoas, onde você está quando você não fala com ninguém. Você já deve ter estranhado como o Google sabe tanta informações sobre você. Então, boa parte disto está relacionado aos metadados. **Aqui nesse link** (em inglês) você pode seguir os passos e verificar o que o *Google* sabe sobre sua vida.

Existem poucas formas de anular metadados, já que eles são necessários nos dados digitais, mas existem algumas formas de "mascarar" estas informações.

Uma delas é usando **diversas identidades**, **ferramentas de anonimato** na comunicação, como ligar de telefones que não estão registrados com seu CPF para outros que também não estão registrados no CPF dos seus contatos.

5. E enviar sms?
É mais seguro?

O *sms* é aquela mensagem de texto que era muito usada antes de existirem os aplicativos como *WhatsApp* e *Telegram*. Mas será que é mais seguro? A resposta é não! *Sms* usa a mesma rede das ligações telefônicas e está exposta ao mesmo tipo de vigilância como o grampo. Se esta for sua única opção, considere a sensibilidade das informações que vocês está enviando. Caso contrário, prefira usar algum aplicativo de mensagens, como *WhatsApp*, *Signal* ou *Telegram*.

CASO 4

*Entrei em contato com duas companheiras para pedir ajuda urgente em um **chat** secreto. Enquanto conversávamos sobre a situação e uma das amigas me recomendava não mencionar detalhes e combinávamos um café, um **chat** não seguro se abriu com uma dessas amigas perguntando estranhamente o que havia acontecido, querendo saber detalhes. Suspeitamos de "boi na linha", encerramos a conversa e, ao tentar contatar essa mesma amiga horas depois, a ligação não completava.*

Estratégia 4

Comunique-se no *chat* do celular com maior privacidade.

O que vou proteger: minhas conversas no *chat*, minha privacidade.

De quem vou proteger: adversários interessados em minhas informações pessoais ou em informações sobre meu ativismo, empresas que comercializam meus dados etc.

TÁTICAS DE DEFESA 4 :

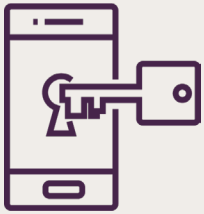
O que fazer imediatamente:

1) Entenda quem está nos grupos de que você participa: se você participa de grupos que atuam politicamente, é essencial que você saiba e confie em quem está dentro dos grupos de *chat*. Saber é poder!

2) Escolha sempre quais tipos de informação e de que jeito você vai falar nos *chats*. Em geral, informações hiper sensíveis são melhores de serem repassadas ao vivo, afinal uma conversa face a face ainda é a forma mais segura de se dialogar sobre alguns temas.

3) Verifique se a pessoa com quem você está falando no *chat* é ela mesma. Afinal, nos *chats* não é possível ver, sentir e escutar quem está do outro lado. Seja desconfiada, pergunte coisas que só a pessoa saberia.

O que fazer para ter mais privacidade?



1. Mas qual é o aplicativo mais seguro? *WhatsApp*, *Telegram* ou *Messenger*?
2. Use identidades diferentes no seu celular
3. Revise as configurações de privacidade dos aplicativos que você usa.
4. Aqui alguns guias: *Whatsapp / Telegram / Instagram / Messenger*

1. Mas qual é o aplicativo mais seguro?
WhatsApp, Telegram ou Messenger?

Antes de tudo, aplicativo mais seguro é aquele onde a gente tem um comportamento seguro, pois, às vezes, os "vacilos" acontecem quando a gente acha que está arrasando e na verdade não está nem perto disto.

Mas se você tomou os cuidados de saber e confiar em quem está nos seus grupos de *chat*, deve estar se perguntando qual *app* escolher para falar com suas companheiras. Aqui vamos falar um pouco dos prós e contras de alguns *apps* na intenção de ajudar na nossa escolha.

1 - *Whatsapp*

Prós: é um dos aplicativo mais usados, usa a **Criptografia fim a fim**, criptografa mensagens, imagens e voz.

Contras: não tem o código aberto, portanto, é como se fosse um bolo em que não se sabe todos os ingredientes; é da mesma empresa do *Facebook* e centraliza um monte de informações sobre você; pertence a uma empresa e vende seus dados na troca de deixá-la usar seus serviços.

2 - *Telegram*

Prós: os grupos e canais são muito interessantes; *stickers* (adesivos, figurinhas) maravilhosos. Afirma que não comercializa seus dados, pois é uma empresa que foi fundada **através de uma herança**.

Contras: não criptografa fim a fim as mensagens de *chat* comuns, apenas aquelas no *chat* privado; não é totalmente de código aberto, é como se a gente soubesse a receita do bolo, mas não da cobertura.

3 - *Messenger*

Pró: alguns contatos usam somente messenger.

Contra: não é criptografado fim a fim por padrão e em todos dispositivos;

Se a sua única opção são esses aplicativos, talvez usar *Whatsapp* com uma boa configuração de segurança seja a melhor escolha porque o sistema de criptografia do aplicativo é mais seguro. Caso contrário, considere instalar o *Signal*. O *Signal* é um aplicativo que usa criptografia fim a fim em todas suas comunicações. Não é comercial, é de código aberto (até que enfim o bolo, mostrando todos

os ingredientes) e foi feito especialmente para pessoas interessadas em oferecer maior privacidade para as que sabem o quanto isto é importante.

Para usar o *Signal*: baixe o aplicativo na loja de apps do seu celular e configure a sua segurança.

Uma opção que vem agradando muito é o *Wire*, outro aplicativo que encripta suas informações fim a fim, é de código aberto e permite a criação de grupos e ligação de áudio de grupo. A principal diferença entre este *app* e o *Signal* é que o *Wire* não requer cadastro de telefone para adicionar os contatos. Os contatos podem ser identificados e acionados somente com o "apelido". Isto pode ser bom no caso em que você não deseje colocar na sua agenda contatos que não quer identificar.

2. Use identidades diferentes no seu celular

Às vezes, não conseguimos saber todas as pessoas que estão em grupos de que participamos, ou para os quais nos convidam e/ou nos procuram em aplicativos através dos nossos nomes. Assim, ter identidades diferentes é essencial para nossa vida digital e pode ajudar a nos protegermos nessas ocasiões.

Algumas dicas rápidas:

a) tente registrar a sua conta do celular (*Google Play* ou *iCloud*) com um e-mail que não seja o seu oficial.

b) mude o seu *nick* (apelido) e não coloque fotos reconhecíveis nos seus perfis.

3. Revise as configurações de privacidade
dos aplicativos que você usa.

Tente seguir esses conselhos para ter mais privacidade nos seus *chats*.

4. Aqui
alguns guias:

WHATSAPP

- **privacidade**
- **como usar a criptografia do *whatsapp***

TELEGRAM

- ***chat* secreto**
- **privacidade**
- **senha na tela**

INSTAGRAM

- **alterar perfil para modo privado**

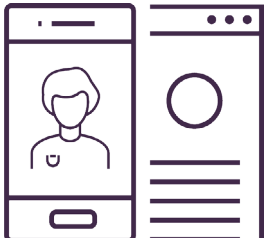
MESSENGER

- **como usar criptografia na mensagem**

PARAR A ESCUTA

- **bloqueio de escuta no facebook**
- **signal**

Redes Sociais



CASO 1

Resolvi postar uma foto no Facebook *junto com um texto falando da minha autoestima como mulher negra, gorda e lésbica, incentivando outras mulheres a amarem seus corpos. Em menos de 24 horas, meu* post *tinha quatro mil comentários onde homens me xingavam e agrediam com discursos carregados de racismo e gordofobia. Uma ataque em massa de homens que participam de fóruns misóginos e de direita foi organizado contra mim, mas apesar de alguns comentários positivos de outras mulheres, a ação dos racistas continuou. Depois de um grande número de denúncias realizadas na minha foto, denúncia essa realizada em massa, o* Facebook *desativou minha conta por quatro dias.*

TÁTICAS DE DEFESA 1 :

O que fazer imediatamente:

1) Tente se acalmar: respire, tente acalmar seu pensamento e aliviar seu estresse usando técnicas de relaxamento.

2) Cheque a privacidade das suas redes sociais e bloqueie os acessos a postagens e mensagens de desconhecidos (veja mais informações a seguir).

Estratégia 1

Entenda como lidar com a violência *on-line* nas redes sociais (misoginia, racismo, lesbofobia, transfobia e afins).

O que vou proteger: meus perfis em redes sociais, minhas informações pessoais, meu ativismo, meu estado psicológico após um ataque.

De quem vou proteger: de pessoas que queiram me impedir de seguir adiante com minha causa (machistas, racistas, facistas, transfóbicos, lesbofóbicos etc.).

O que fazer para segurar a onda e virar o jogo:

1. Rede de apoio: você não está sozinha!
2. Não deixe brechas
3. Denuncie
4. Avise quem você acha importante saber
5. Crie sua estratégia de comunicação

1. Rede de apoio:
você não está sozinha!

No caso de ser uma ativista que atua de forma individualizada na internet: você não é obrigada, e não deve, lidar com os ataques sozinha. Ler todas as postagens ofensivas pode fazer muito mal para você, e pode ser um redemoinho que tem o poder de afogar sua autoestima.

Passar por isto não é necessário e pode ser muito doloroso. Recomendamos que você chame uma companheira, amiga em que você confia, ou contate uma rede de apoio para ajudá-la nessas horas.

Redes de apoio podem ser suas redes de contatos próximos ou canais em que você confia. Esta rede pode lhe dar suporte e ajudar você a segurar a onda dos ataques.

Você pode chamar também uma amiga de confiança e pedir que ela a ajude a gerenciar suas redes sociais para lhe dar um alívio durante os ataques mais pesados.

Juntar-se com as outras ativistas: Estar juntinha é melhor do que só na *bad*, né? Assim como os grupos "baixo astral" estão organizados, nós também estamos. Somos várias espalhadas por todo o Brasil e dispostas a cuidarmos umas das outras. Então busque uma rede de apoio mais próxima de você e converse. Grupos como as meninas do #MaisAmorEntreNós, #TamoJuntas e outras mais podem ajudá-la. O importante é não achar que está só. Dê cá um abraço!

2. Não
deixe brechas.

Troque suas senhas e verifique se as configurações de segurança para acessar suas contas usam dupla autenticação como mensagens para celular ou perguntas de confiança.

Aqui nesse ***link*** tem dicas para arrasar nas senhas, e aqui dicas para ativar a dupla autenticação nas redes: ***Facebook***, ***Twitter***, ***Gmail***.

Verifique se você tem informações dando sopa por aí que podem ser descobertas por pessoas mal intencionadas. Uma forma é verificar nas redes sociais **quais informações suas estão visíveis para o público**. Lembre-se também de verificar se a **lista de seus contatos está visível ou não**, pois ela pode revelar muitas coisas sobre você e suas relações. Outra forma é procurar nos buscadores populares como *Google* e *DuckDuckGo* o que mais está visível para quem for atrás de suas informações e tentar melhorar suas defesas no possível.

Verificar essas informações é muito importante, pois hoje essas ferramentas de busca centralizam um monte de informações que nem a gente sabe que está lá! Por isto, é essencial fazer essa busca e tentar tirar do ar qualquer tipo de informação desnecessária sobre você, especialmente as informações que expõem seu endereço, número de telefone, documentos...

Alguns dados você não vai conseguir apagar, mas talvez consiga alterar! Às vezes, é mais fácil entrar em contas antigas de redes sociais "mortas" como *Myspace* ou *Fotologs* e editar todas as informações públicas como "*nicks*" (apelidos), nome, idade, endereços... Você pode alterar para informações e interesses totalmente falsos.

Se você tem um *site* ou página *web*, é bom também verificar se o domínio do site está revelando informações sobre seu endereço e dados cadastrais. Para fazer isto, você pode fazer **uma consulta aqui**.

Outra boa dica é esconder suas informações privadas nas redes sociais, **veja aqui** como fazer isto no *Facebook*.

3. Denuncie!

Um dos problemas da internet é que grandes *sites* são como grandes cidades onde algumas empresas ditam as leis. Teoricamente, porque não é assim que a banda toca ou deveria tocar. Na prática, mesmo, pense que um *site* é sistema que fica instalado em um **servidor** (um grande computador ligado à rede) e pode ser acessado por um endereço de internet (IP). Este endereço tem uma correspondência física, já que este computador e esta conexão de rede estão fisicamente em algum lugar do mundo. E, portanto, o *site* está sujeito às leis daquele lugar do mundo em que está sediado, e a pessoa está sujeita às leis do lugar do mundo de onde acessa este site.

Diante disso, lembre-se: apesar de não termos ainda uma lei abrangente de internet e crimes virtuais no Brasil, as leis vigentes para crimes valem também para qualquer *site* que preste serviço no Brasil, sendo assim responsável por responder legalmente a sua sede administrativa. **Ou seja: crime continua sendo crime, não muda nada se é a internet ou não.** E com relação a páginas derrubadas propositalmente sem um motivo legítimo, estamos falando de difamação e injúria. Por isto, cabe denúncia ao Ministério Público Federal (MPF), caso as pessoas envolvidas sejam conhecidas.

Para ajudar nessa tarefa nunca simples de denunciar pessoas, ainda mais quando nem sempre conhecemos todas as pessoas culpadas, dois canais de apoio existem no país: um é o **#humanizaredes** criado pelo Governo Federal, e outro, já atuando desde 2007 no Brasil, é a **Safernet**, uma organização não governamental que atua diretamente com o MPF e a Polícia Federal no encaminhamento de denúncias . E como estamos falando de leis, buscar apoio de advogadas e juristas é muito válido antes de pisar em um terreno desconhecido.

Alguns outros links para denúncias mais específicas:

- **Denúncia no Youtube**
- **Denúncia no Instagram**
- **Denúncia no Twitter**
- **Denúncia “na internet” através do Safernet**
- **Denúncias contra crimes de ódio**
- **Denúncia dentro do Facebook**
- **Informações diversas sobre crimes de violência online contra mulheres**

4. Avise quem você acha importante saber.

Avise as pessoas próximas a você que o ataque está acontecendo e as prepare para as possíveis situações que podem acontecer devido ao ataque, como receber ligações e encomendas na sua casa.

CASO 2

Nosso coletivo tinha um grupo no Facebook *e, por causa do grande número de vezes em que tivemos que lidar com perfis* fakes *(falsos), informações vazadas e ataques de homens machistas, nós decidimos retirar o nosso grupo de aproximadamente três mil mulheres negras do* Facebook *e migramos para outra plataforma, desenvolvendo um* app *para discussões, compartilhamento de informações e outras trocas.*

Estratégia 2

Organize articulações e mobilizações em redes sociais.

O que vou proteger: minhas articulações, as mobilizações organizadas, as pessoas participantes das articulações e mobilizações, minha privacidade.

De quem vou proteger: de adversários interessados em minhas informações pessoais ou informações sobre meu ativismo e do coletivo de que faço parte,, empresas que comercializam meus dados, agressores, machistas, racistas, facistas, transfóbicos, lesbofóbicos etc.

TÁTICAS DE DEFESA 2 :

O que fazer imediatamente:

1) Pense e reflita: não seria melhor mudar de rede social?

2) Se você está certa de que o vazamento aconteceu do seu grupo/comunidade na rede social azul, **faça *backup* de todos os conteúdos**.

3) Depois de guardar todo o conteúdo, se for estatégico para o seu grupo ou coletivo, desfaça a comunidade/*page*/ perfil na rede social e comece a pensar em qual outro espaço vocês conseguem se reunir com mais segurança.

O QUE FAZER PARA SE PROTEGER:

1. Conheça as alternativas para se organizar coletivamente na internet

1. Conheça as alternativas para se organizar coletivamente na internet.

Formar grupos é um babado forte! Somos seres humanos e temos a necessidade e capacidade de nos agruparmos e atuarmos em coletividade. Parece até que foram as redes sociais que inventaram isto, né? *Apois*, não. A real é que precisamos entender o que queremos fazer em grupo para entender onde podemos nos organizar. Então, a primeira coisa é: *" o que eu quero/queremos fazer?"* e então pensar *"onde vamos organizar essa galera?"*.

Então, antes de tudo é bom entendermos que tipo de grupo queremos criar, pois, dependendo das informações que vamos discutir dentro dos grupos, podemos escolher plataformas e configurações diferentes para definir o tipo de proteção e divulgação que queremos dar às informações que estarão lá dentro.

Talvez estar em uma plataforma como *Facebook* seja necessário para que você consiga comunicar com as pessoas e segmentos que você quer alcançar. Então é bom entender se o grupo será: público (aberto para tod@s); privado (aparecerá nas buscas mas será fechado) ou secreto (não aparecerá nas buscas e será fechado). Veja aqui **nesse link** mais informações sobre os tipos de grupos.

O *Telegram* vem sendo muito usado para grupos por ser um *chat* que tem muitas pessoas cadastradas e é acessível para diferentes públicos. Se for usar esta plataforma, **entenda a diferença entre grupos, supergrupos e canais**.

Lembre-se sempre que essas plataformas podem ler suas informações. Por isto, não recomendamos usá-las para compartilhar informações privadas e sensíveis, pois estas podem ser acessadas pelas empresas e não estão criptografadas fim a fim.

Já o *WhatsApp* se propõe a criptografar as mensagens de grupos, desde que tod@s do grupo tenham celulares habilitados com criptografia. Mesmo assim, recomendamos cautela, pois como falado antes, este aplicativo é uma receita de bolo em que não conseguimos ver os ingredientes, e em que não podemos confiar 100%.

Para ter mais segurança, privacidade e confiança nos aplicativos e serviços, recomendamos as seguintes opções:

- Grupos no *Signal*: Para criar os grupos, instale o *app* e oriente seus contatos para fazerem o mesmo. Depois clique nos "três pontinhos" do canto superior direito e crie o "Novo Grupo". Mais informações do aplicativo no capítulo 4.02.

- Grupos no *Wire*: Para criar os grupos no *Wire*, instale o *app* e peça para suas amigas fazerem o mesmo. Entre nas suas "Conversas" e clique no símbolo de "pessoazinha" no canto esquerdo inferior. Depois selecione seus contatos e dê um nome ao grupo.

- Grupos no *WeRiseup*: O *WeRiseup* é a uma plataforma do coletivo de servidores ativistas *Riseup*, que se trata de uma plataforma anticapitalista e segura que provê serviços para grupos ativistas. Os grupos podem criar uma sessão privada para conversar sobre assuntos mais secretos. Para saber mais informações de como criar os grupos, **acesse este link**.

- Outra opção, se o seu grupo tiver uma integrante que entenda de servidores, é instalar uma plataforma de rede social, como o ***HumHub*** - Para mais informações, recomendamos contatar as *sys-adminas* ***Vedetas***.

CASO 3

Comecei a conversar com um garoto que conheci por um aplicativo e enviei pra ele fotos minhas. Nos encontramos uma vez e eu desisti da paquera, e a partir de então ele começou a me ameaçar e me perseguir. O cúmulo disso foi ele fazer uma fotomontagem com as imagens que enviei e compartilhar com meu atual namorado e ameaçar enviar aos meus amigos.

Estratégia 3

Se proteja da vingança pornô.

O que vou proteger: minha privacidade, minha sexualidade, meu direito à nudez consentida.

De quem vou proteger: agressores, machistas, racistas, facistas, transfóbicos, lesbofóbicos etc.

TÁTICAS DE DEFESA 3:

O que fazer imediatamente:

1) Não fique só, converse com grupos de apoio ou com as pessoas próximas a você.

2) Proteja seus contatos: a vingança só vai ser cumprida se a pessoa atingir as pessoas que estão próximas a você. Assim que a ameaça da vingança acontecer, tente conversar com essas pessoas, se possível. Em todo o caso, **esconda sua lista de contatos do *Facebook***.

O que fazer para se proteger e virar o jogo:

1. Entenda, a culpa não é sua
2. Conheça o guia *Nudes* Seguros
3. Saiba como denunciar
4. Como andam as leis?

1. Entenda,
a culpa não é sua!

A sexualidade humana sempre foi controlada e julgada, principalmente a que se refere ao corpo feminino, e não é estranho perceber que as narrativas sobre vingança pornô são na sua maioria paternilizadoras e deslocam a culpabilização para a vítima, que é quase sempre uma mulher.

Quando um ***nude*** é usado para chantagear, ameaçar ou agredir, trata-se de uma violência que atinge o corpo e a liberdade sexual da mulher, pois o corpo é objetificado e violentado, também a sexualidade feminina que é considerada "perversa" e "obscena", e assim culpabilizada.

É muito importante saber que a culpa de uma vingança pornô não é sua. O fato de você ter exercido a sua sexualidade mandando uma foto não é errado. Não se deixe cair na culpa dos outros.

2. Conheça o guia
Nudes Seguros.

Existem formas de exercer sua sexualidade e liberdade sem se expor ou se colocar em risco. É fundamental conhecer o ***Guia de Nudes Seguros*** e ficar mais segura a próxima vez que for fazer e mandar aquela foto linda.

3. Saiba como
Denunciar.

Denunciar a agressão é importante. Recomendamos ler os passos listados aqui no ***"Manda Prints"*** para saber como proceder caso seja necessário.

Lembre-se que você pode pedir ajuda para as amigas fazerem a denúncia, caso a situação esteja muito estressante para você. Os passos para registros continuam sendo os mesmos.

4. Como
andam as leis?

Atualmente uma vingança pornô entra como julgamento de injúria e dano moral, requerendo um processo feito através de um acompanhamento com advogadas/os ou defensoria, o que é demorado ou custoso. Como pena, pode-se conseguir indenizações e multas, o que é realmente fraco e insuficiente para a situação pela qual as mulheres têm que passar.

Apesar disto, é importante denunciar, claro, respeitando nossos limites. As denúncias servem tanto para tentar alguma proteção e punição, quanto para ajudar que as leis mudem e possam atender de fato às situações em cenários futuros... Porque a visão em que essas coisas não vão ter outro tipo de atendimento é terrível demais.

O PL 5555/2013 (ainda em tramitação no Congresso Nacional, em junho 2017) prevê mudanças na Lei Maria da Penha para adicionar o crime digital contra a honra da mulher. Apesar de ser ótimo que um PL sobre o assunto esteja tramitando, o fato de ser uma modificação na Lei Maria da Penha preocupa algumas pessoas pois abre precedente para mudanças em uma lei que é tão importante para a segurança das mulheres. Ainda assim, o fato que mais desagrada as advogadas que estão acompanhando a tramitação do PL é que este propõe uma tipificação criminal vinculada à injúria e não à violência sexual. Sendo assim, os processos continuarão a ser lentos e custosos, e sobretudo as violências não serão reconhecidas.

Apesar de todos os "poréns", a luta para que esse e mais PLs sejam de fato aprovados ainda é uma causa para nós, mulheres, que sofremos toda vez que uma mulher é colocada em situação de exposição e, sobretudo, toda vez que a nossa sexualidade é usada para acabar com nossa liberdade de viver em paz.

CASO 4

Meu coletivo acolheu um novo militante que participava ativamente de reuniões, encontros e protestos. Depois de sermos perseguidos e presos nos protestos de 2013, descobrimos que esse companheiro era um infiltrado, que mantinha um perfil fake*, que assediava mulheres e colhia informações para entregar planos e ações do movimento.*

Estratégia 3

Sem P2 (infiltrado) na minha rede social.

O que vou proteger: minha privacidade, meu ativismo, meu direito de ser uma pessoa política, meu bem estar emocional.

De quem vou proteger: de opressores, adversários que têm interesse no meu ativismo, em sencionalismos e na criação de histórias midiáticas etc.

TÁTICAS DE DEFESA 3 :

O que fazer imediatamente:

1) Se você está desconfiada de alguém, converse com a pessoa mais experiente do seu coletivo. Junt@s vocês podem chegar a alguma conclusão e assim conversar com todo o grupo.

2) Se vocês ainda têm dúvidas, pesquisem esse integrante: vão atrás da história passada, tentem fazer uma linha do tempo regressiva que logo acharão alguma brecha, se ele for p2 (infiltrado), claro.

COMO ME PROTEGER E ME SENTIR SEGURA?

1. Como acontecem os monitoramentos de ativistas nas redes sociais?

Nos últimos anos, estamos acompanhando monitoramentos em redes sociais feitos através de uma prática chamada OSINT – *Open Source Information*, que são análises feitas a partir dos perfis públicos e *timelines* das redes mais conhecidas, como *Facebook*, *Twitter* e *Instagram*. Como são dados teoricamente públicos, não existem leis que regulamentem essa prática, principalmente essas vigilâncias em movimentos sociais.

Os agentes "infiltrados" são regulamentados pelas leis que investigam organizações criminosas (12.850/13) e tráfico de drogas (11.343/06). Recentemente foi aprovada uma lei que regulamenta a prática no ambiente digital para investigar casos de pedofilia.

Contudo, criar uma identidade virtual falsa – que não tem o objetivo de tirar proveito ou prejudicar uma pessoa – não é ilegal, ainda mais se for um perfil falso que está acompanhando suas informações públicas. Porém, se forem informações privadas, a ação pode ser considerada ilegal se não autorizada.

Mas... como sabemos, as leis podem dizer uma coisa e a vida, outra... Por isto, vale ficar de olho aberto n@s "amig@s" que se dizem "amig@s" e são "inimig@s".

2 . *Mucho* amigos
igual a nada amigos.

"*50 amigues em comum? Claro que eu posso adicionar! Só conhece gente firmeza!*"
Uma troca de olhares rapidinha, um clique, pronto. Quando falamos em redes e mídias sociais, fazer amizades pode ser algo muito fácil, uma relação de confiança entre amigos de amigos. Porém, justamente pela facilidade, este é um meio muito comum de chegar até pessoas fragilizadas. É fácil e rápido criar um perfil, ou mesmo mudá-lo, para ter interesses comuns e participar de coisas que todas as pessoas-alvo de forma insuspeita. E aí, aquela pessoa amiga da amiga se revela o ponto fraco da sua segurança na internet.

3. Cautela e uma perguntadinha
não fazem mal a ninguém.

Paranoia? Talvez não, se você for a administradora de uma página ou atuar em um contexto político que a exponha publicamente. Por isto, faça o exercício de observar sempre que possível e perguntar diretamente às pessoas de sua confiança sobre a legitimidade de alguém, caso desconfie. E, para todos os efeitos, procure evitar adicionar pessoas que você não conheça pessoalmente. Lembre-se: rede social é sobre pessoas do seu círculo social. E popularidade e alcance nem sempre estão relacionados à sua quantidade de amig@s e seguidor@s. Existe muito *marketing* e estatística por trás do que faz suas palavras e imagens chegarem a mais pessoas.

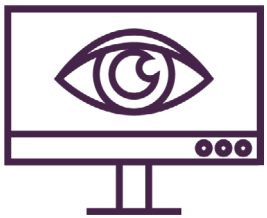
4. Configurações de privacidade:
10 minutos que podem fazer a diferença!

Tente dedicar um tempinho para configurar suas políticas de privacidade. Configurar bloqueio de mensagens de usuários que não adicionaram você, criar grupos de usuários que podem ver suas postagens (sabe aqueles de "amigos" e "conhecidos"? Eles podem evitar grandes dores de cabeça para enviar mensagens apenas para determinadas pessoas) e sempre dar uma olhada na lista de pessoas bloqueadas (para ver mudanças de nome, e inclusive alertar pessoas da sua rede de confiança sobre essas mudanças repentinas de identidade). São práticas que tomam dez minutos e salvam muitos momentos de constrangimento pessoal.

5. Ninguém é
uma pessoa só.

As grandes redes e mídias sociais pregam políticas de integridade como a conturbada "política do nome real" (que prejudica muita gente real também) e a ideia de que sua confiabilidade está ligada a ter um único perfil com informações pessoais atualizadas o tempo todo. Mas isto não é verdadeiro nem na vida real! Quem disse que a sua pessoa privada é igual à sua pessoa política, ou à pessoa profissional? Por isto, caso você tenha uma identidade pública ou profissional (que inclusive são tão íntegras quanto você mesma), considere a ideia de ter um perfil privado só seu e das pessoas mais próximas, realmente conhecidas, e fazer outro perfil, para administrar sua página e receber pessoas fora do círculo. Não só você se torna capaz de criar um filtro mais elaborado do círculo de pessoas ao redor, como também evita situações como a derrubada da sua página por conta de um bloqueio proposital ao seu perfil pessoal, por exemplo. Pode se apropriar do "dividir para conquistar", é pra mulher e travesti e ***não-binarie***[10] também.

[10] Pessoas **não-binárias** ou **nãobinárias** são pessoas cujo gênero não é nem 100% masculino e nem 100% feminino. Isso inclui: Pessoas com múltiplos gêneros, de uma vez só ou um de cada vez, mudando de tempos em tempos; Pessoas que são parcialmente, mas não totalmente, de algum gênero, mesmo que esta parte seja de um gênero binário; Pessoas que não possuem gênero, que se sentem à parte do conceito de gênero, ou que sentem que transcendem gênero; Pessoas que não entendem gênero, que não entendem o próprio gênero, ou que não se importam com o próprio gênero; Pessoas cujos gêneros existem, mas que não são nem o masculino nem o feminino; Pessoas cujos gêneros são relacionados à masculinidade, à feminilidade, ao masculino, ao feminino, ou a ambos os gêneros binários, mas que não podem ser caracterizados como homem ou como mulher; Pessoas que não são 100% homens e nem 100% mulheres por causa de neurodivergência, trauma, intersexualidade, espiritualidade, cultura, orientação sexual, orientação romântica, e/ou outras experiências de vida; entre outras possibilidades. Disponível em: http://orientando.org/listas/lista-de-generos/nao-binarie/. Acesso em: 2 out. 2017.



CASO 5

Uma ativista escreveu um texto há um tempo para um site onde possui uma coluna. Este texto é um dos mais lidos até hoje e de vez em quando volta a ter picos de acesso, justamente por conta de haters. *Recentemente, uma página compartilhou esse texto como transfobia e discurso de ódio, provocando comentários piores ainda e, apesar de ter sido denunciada, a página permanece ativa nas redes sociais*

Estratégia 5

Não deixe que a página que caiu derrube você e seu coletivo.

O que vou proteger: minha privacidade, meu ativismo, meu direito de ser uma pessoa política e de me posicionar politicamente, meu bem estar emocional, nosso coletivo.

De quem vou proteger: de opressores, adversários que têm interesse no meu/nosso ativismo, em histórias midiáticas etc.

TÁTICAS DE DEFESA 5 :

O que fazer imediatamente:

1) Fique calma! Se você tem um serviço de servidor, entre em contato com ele e certifique-se de que você caiu e por que caiu. Peça para que o modo de segurança do seu *site* seja ativado e, caso conheça, peça ajuda a outras mulheres que entendam de segurança.

2) Você pode também salvar aquele conteúdo que foi atacado, retirá-lo um tempo do ar e depois subi-lo novamente. Esta tática engana os *haters* (pessoas com discurso de ódio) e coloca o conteúdo em um novo link, podendo livrar você momentaneamente dos ataques.

COMO SE PROTEGER E SE RECUPERAR DE UM ATAQUE

1. Busque suas redes de apoio e converse com o seu coletivo e suas companheiras e amigas
2. Entenda onde reclamar sobre uma página que foi derrubada
3. Entenda sobre políticas de privacidade

1. Busque suas redes de apoio e converse com o seu coletivo e suas companheiras e amigas.

Sabe qual é a vantagem de trabalhar na rede? Ela ser... uma rede!

Parece uma péssima piada, mas a verdade é que quando estamos em uma situação de risco ou pressão, esquecemos muitas vezes que temos uma grande rede com muitas outras pessoas com diversas experiências a dividir. Não apenas pessoas que entendem de segurança digital: pessoas que já passaram pelo mesmo que você. Estas, muitas vezes, possuem dicas valiosas para dividir. E claro, com uma ajudinha *dazamiga* e de conhecimentos de táticas de defesa e contra-defesa, você evita muita coisa. Nas sessões anteriores, falamos sobre criar novas identidades, configurações de privacidade, identidades coletivas – onde você divide a responsabilidade com um grupo de pessoas, e isto não é só útil para páginas: você pode usar em perfis pessoais e ajudar a camuflar os endereços de acesso entre múltiplas pessoas, uma técnica que chamamos de “cortina de fumaça”.

Mesmo sem o controle da plataforma, o controle sobre a sua identidade é exclusivamente seu. Mas como dizem por aí: quando duas pessoas dividem uma ideia, saem com duas.

2. Entenda onde reclamar
sobre uma página que foi derrubada.

Algumas vezes, nossas formas de falar contra a opressão são utilizadas também contra nós de forma mal intencionada. Sabemos que nem sempre páginas denunciadas por conteúdo violento ou discurso de ódio são consideradas impróprias, e da mesma forma, páginas utilizadas para espalhar conteúdos feministas e anti-discriminação como um todo são desativadas por denúncias infundadas.

Para tomar uma ação direta e entrar em contato sobre uma página que foi derrubada dessa forma, clique no ícone de interrogação (?) ao lado das notificações do seu perfil (Ajuda Rápida) e siga as opções: **Relatar um problema > Algo não está funcionando > Páginas**. Descreva detalhadamente os acontecimentos e os detalhes de como sua página foi denunciada de forma mal intencionada, incluindo capturas de tela marcando a caixa "*Incluir uma captura de tela no meu relatório*" e usando o botão "*Carregar capturas de tela*".

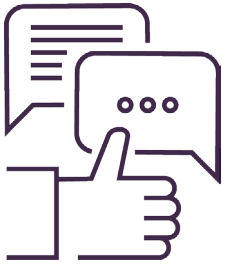
Além disso, faça barulho nas redes, exponha o caso, sempre lembrando dos cuidados para não expor a si ou a pessoas e informações que possam causar complicações jurídicas. Como dito em outras seções da Guia, quando envolver leis, não hesite em consultar advogadas e coletivos de juristas caso tenha dúvidas do que deve ou não jogar na internet. E sempre que possível, saia do radar das mídias sociais: publique em blogs pessoais e busque apoio nos coletivos de blogueiras feministas. Não se isole!

3. Entenda sobre
políticas de privacidade.

É muito chato. Muito. Mas na maioria dos casos, compreender as políticas de privacidade e os termos de serviço – aqueles que muitas vezes nunca lemos e só clicamos em "Aceito" – é a peça fundamental de defesa e contra-argumento em casos de ataques. Muitas vezes, estes ataques estão baseados em coisas que você disse em um perfil pessoal (e não em sua página pública) e em brechas dos termos das mídias sociais que constantemente esquecemos. Mas nossos detratores lembram o tempo inteiro. Lembra das minas fazendo teste postando a palavra "sapatão" e sendo denunciadas? Pois é. Lembramos inclusive de amigas que usaram a palavra "viado" dentro de um contexto (denunciando transfobia) e sendo denunciadas por... homofobia! Pode? É péssimo, mas pode. Porque é esta a brecha usada para denunciar, já que a máquina não entende contexto (e nem sempre os seres humanos fazem questão de entendê-lo também).

Portanto, o que você precisa lembrar é que as empresas por trás das grandes mídias e redes sociais não estão a seu favor. São empresas, logo possuem interesses financeiros. E não é difícil lembrar de que lado está o dinheiro quando não temos nem igualdade de salários, né? E como toda mídia com poder econômico, são capazes de controlar o que você diz. Apesar da projeção que elas dão, como ferramentas de alcance de pessoas com os mesmos objetivos, meios como o *Facebook* não são neutros o bastante para serem considerados plataformas de articulação política. Não quer dizer que você precise se curvar, mas é importante pensar em como trabalhar e subverter a mensagem.

CONTAS, COMUNICAÇÃO E ARQUIVOS MAIS SEGUROS



CASO 1

Fiquei assustada quando percebi que poderia levar menos de um minuto para quebrar minha senha usando um site *da internet, e que com isso, podia ter todas as minhas contas invadidas. Tinha acabado de publicar um matéria polêmica no meu blog e não estava pronta para encarar uma possível invasão da minha conta de e-mail.*

TÁTICAS DE DEFESA 1:

O que fazer imediatamente:

1) Avise suas amigas e seus contatos mais próximos que a bomba está para vir e que você vai precisar do apoio del@s em breve.

2) Revise a privacidade da sua linha do tempo das redes sociais. Não deixe brechas para acharem fotos suas, ou para que sua *timeline* fique cheia de "recados" de uma hora para outra. Mais informações na **Estratégia 1**, na sessão de Redes Sociais.

3) Mude suas senhas e revise suas senhas de e-mail e outros serviços *on-line*.

Estratégia 1

Saiba como se preparar quando você sabe que algo que te deixará em exposição está para acontecer.

O que vou proteger: minha privacidade, acesso aos meus emails e informações pessoais, acesso as minhas contas de redes sociais.

De quem vou proteger: adversários interessados em minhas informações pessoais ou informações sobre meu ativismo, agressores, machistas, racistas, facistas, transfóbicos, lesbofóbicos etc.

COMO PROTEGER MINHAS CONTAS?

1. Como criar e manter senhas boas?
2. O que mais posso fazer para melhorar a segurança do acesso as minhas contas?
3. Cheque suas ligações na nuvem e seus rastros digitais
4. Prepare suas redes sociais
5. Tenha uma rede de apoio perto de você
6. O que mais posso fazer? Quais são meus direitos?

1. Como criar e manter senhas boas?

Criar senhas é sempre uma tortura. Lembrar delas? Piorou. Mas isto não é uma desculpa nos dias de hoje. Por muito tempo usamos senhas fáceis por medo de perdê-las, esquecê-las e encorajadas pela dificuldade de trocar senhas nos *sites* e sistemas que usamos ("*botei aquele lembrete de 72 dias, mas onde troca a senha mesmo?*"). Hoje, temos muitas ferramentas a nosso alcance. Como por exemplo, os aplicativos de cofre de senha. Você deve conhecer aquele da internet, o *LastPass*. Mas você já parou para pensar que está guardando sua senha num lugar desconhecido na internet de uma empresa que diz garantir sua privacidade mas, mesmo assim... Parece seguro? Não.

Por isto temos soluções *off-line* (que você instala no computador ou no celular), como o ***KeepassX*** (*Windows*, *Linux*, *MacOS*) ou o *Minikeepass* (*Android*, *iPhone*). Você só precisa criar um banco de dados com uma única senha para guardar todas as suas outras senhas. O melhor de tudo: ele ajuda a criar senhas fortes com um gerador automático! O guia abaixo fala sobre como instalar no *Windows* mas o funcionamento é igualzinho para *Linux* (também tem um guia) e *Mac*: ***https://securityinabox.org/pt/guide/keepassx/windows/***

> *"Tá, tudo bem, mas eu ainda preciso decorar uma senha segura. E como eu posso criar esta senha super segura que protege todas as outras?"*

Uma senha ideal é uma senha com pelo menos 20 caracteres (letras, números, símbolos), alternando maiúsculas e minúsculas. Por que isto é importante? Que tal testar uma senha simples (não teste a sua diretamente, mas uma parecida) **neste site** neste *site* que diz quanto tempo leva para quebrar uma senha?

Assustou? Então... Porém, já há algumas décadas um pesquisador desenvolveu uma ideia: uma boa senha é uma boa frase, com letras maiúsculas e minúsculas, espaços e pontuações. Fácil de lembrar, segura o bastante. Essa técnica foi chamada de *diceware*, ou ***dadoware*** como conhecemos aqui. E tem um guia inteiro traduzido para o português. Mas a ideia é esta: junte palavras diversas e que você possa memorizar facilmente em uma frase. Já melhora muito sua vida!

2. O que mais posso fazer para melhorar a segurança do acesso as minhas contas?

Falamos um monte sobre senhas. Mas e agora? Só isso basta? A gente sabe que não. Mesmo que você tenha uma senha que leve um bilhão de anos para ser quebrada, ela pode ser descoberta de outras tantas formas. E aí?

Aí que uma das técnicas de segurança mais recentes (não tão recente assim - pra quem já teve conta em banco, lembra do ***token***?) é a autenticação em dois fatores, ou **TFA** (*Two-Factor Authentication*). Ela se baseia em uma das dicas de segurança mais clássicas desde o surgimento da internet: procure acessar suas contas do mesmo computador, ou dos mesmos dispositivos. Aliás, ela ainda é uma dica válida mesmo quando seus sistemas não aceitam a **TFA**, viu? Mas com ela, você garante que, além da sua senha, você só possa acessar uma conta tendo acesso ao número de acesso (*token,* mesma coisa), que é dado por outro dispositivo, geralmente o seu celular. Assim, além de saber a sua senha, a pessoa invasora teria que ter acesso ao seu dispositivo pessoal para saber o código (que é gerado aleatoriamente a cada acesso).

A maior parte das mídias sociais e aplicativos de *chat* modernos (assim como *sites* de serviços, especialmente financeiros) aceitam a autenticação em dois fatores hoje em dia. O inconveniente é que, se você perder o celular, você vai ter que acessar o suporte desses aplicativos diretamente para resetar esta configuração. Caso você se encontre em uma situação em que o risco de perder o celular é iminente, considere: o seu acesso é mais importante que a possibilidade de acessarem sua conta? Se você se sentir muito segura sobre não estar sendo perseguida virtualmente, mas fisicamente existe um risco e você precisa do acesso a uma rede específica, considere desabilitar esse tipo de autenticação apenas para aquela rede para evitar transtornos. Mas pense bem: às vezes, é melhor lidar com o transtorno do que correr o risco de entregar suas informações a outras pessoas.

3. Cheque suas ligações
na nuvem e seus rastros digitais.

É bem comum ouvir alguém dizer que é muito fácil encontrar informações sobre uma pessoa na internet. Bem, não é uma mentira tão absurda. Mas o fato é que se você chegou até aqui, é possível que já saiba um monte de coisas que tornam a vida de uma pessoa "*zoião*" mais difícil. Por exemplo, se você checou as configurações de privacidade das suas redes, já ganhou uns pontos. Separou público de pessoal, mais alguns. Mas, às vezes uma coisa ou outra passa. Quem nunca achou que não seria problema deixar um número de telefone ou endereço de e-mail público, "vai que alguma amiga precise". E quando isto acontece, temos algumas ferramentas enxeridas que podem nos encontrar facilmente, como o **Pipl**. Por isto, uma boa prática é deixar o menor número de informações pessoais possíveis disponíveis. Como a internet é pra sempre, ainda vai levar um tempo pra essas informações caírem no esquecimento. Mas começando agora você já começa a deixar muito menos rastros perdidos por aí.

Esse *site* (em inglês e espanhol) dá uma mãozinha em explicar e mostrar quantos rastros você deixa na internet, e que rastros são estes. E explica coisas como ***cookies***, ***trackers*** e mais um monte de termos (que você também vai encontrar na sessão "**Entenda bem, meu bem**", pode deixar).

Uma das dicas ótimas que você encontra lá é sobre ter contas de e-mail secundárias para registrar seus *apps* e sistemas, coisa que além de ajudarem você a ter uma caixa de e-mail com bem menos *spam* evita que esses *trackers* liguem sua identidade ao seu e-mail. Pensou que era só o perfil da rede social que ficava na mira, é? Vai vendo. Além do mais, usar uma segunda conta pra registrar o *Google* no *Android* ou a *App Store* do *iPhone* ajuda em várias outras coisas: evita que liguem seu e-mail a seu número de celular, permite que você tenha o *backup* dos seus contatos em outra conta separada, caso a sua conta principal seja comprometida... Viu, várias fitas.

Outra coisa que nunca é demais lembrar: faça uma limpeza no navegador com alguma frequência. Semanal é uma boa, não precisa ser tão paranoica. Até porque, se precisar navegar sem gravar nada, você pode usar o recurso da janela anônima. Mas presta bem atenção: janela anônima não é igual **navegação anônima**, tá? Janela anônima evita que você guarde histórico de navegação, ***cookies*** e ***cache*** de páginas. Só isto. Não esconde seu **endereço de internet (IP)** nem faz você ter uma "capa invisível" (dentro dos limites que a internet possui). Isso é outro *migo*, o ***Tor,*** que você vai baixar **aqui**. Lá na "**Entenda bem, meu bem**" você vai encontrar mais detalhes sobre como este tal de ***Tor*** trabalha na causa e porque ele tem este nome.

É muita coisa, né? Mas tem mais uma: sabe aquelas contas de *site* da internet que você usou duas vezes na vida? Lembra daquele ask.fm que você fez há uns três verões atrás e nem lembra que existe? Então, esses lugares sabem muita coisa de você. Mas como deletar essas contas? Essa resposta quem nos dá é o ***Just Delete Me***. Você vai ver que nem todos os *sites* são tão amigáveis pra deletar uma conta. Alguns são impossíveis, até. Mas essa é a melhor referência que você vai encontrar sobre como tirar seu nome de uma das milhões de encruzilhadas da internet.

4. Prepare suas redes sociais.

Se você leu direitinho as táticas de defesa 5 e 6 das redes sociais, já está espertíssima. Mas não custa nada relembrar: faça uma ronda nas suas redes sociais e mantenha suas informações o mais privadas possível. Quem merece informação sua é gente em que você confia. O resto pode passar bem longe.

O *Facebook* tem **uma página** toda na Central de Ajuda para privacidade da conta.

Na página de **ajuda do *Twitter*** (mude a linguagem para português no topo da página), você acha informações sobre *tweets* protegidos e mensagens privadas, que é o que tem pra hoje.

O *Instagram*, uma das redes mais difíceis de tornar mais segura e privada, só tem **página de ajuda** em inglês. Mancada, bora cobrar tradução. Mas tem um bocado de informação que dá pra conseguir com ajuda de um tradutor.

Pelo menos essas três famosinhas vale a pena linkar aqui. Mas lembre-se sempre de procurar a página de ajuda de toda e qualquer rede para encontrar informações sobre como configurar sua privacidade. E, se não tiver, entre mesmo em contato com o suporte, eles têm obrigação de responder você. E se a resposta não for legal, já sabe de qual site você não será mais usuária né? Por favor...

5. Tenha uma rede de apoio perto de você.

Outra coisa que você deve saber mas não custa falar de novo: a sua rede de amigas e amigos para valer você já fez fora da internet. A internet é só um meio para aproximar e criar mais elos com essas pessoas, e esta é a importância de redes de apoio. Saiba as pessoas com quem você pode contar na hora do aperto. E estar perto pode ser pela internet também: crie grupos privados de comunicação com essas pessoas, se possível em um *chat* seguro como o ***Signal*** ou o ***Wire***. O *Signal* pede que você tenha a pessoa gravada nos contatos do seu telefone para poder fazer comunicações. Este é um dos métodos que ele usa pra criar uma rede de confiança. O *Wire*, por sua vez, não depende de

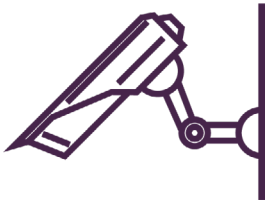
telefone, o que pode ser bom em caso de perda ou daquela pessoa que não pode usar um número agora por algum motivo. E claro: se a coisa não for tão grave assim, um grupo de *WhatsApp* ou *Telegram* já fazem o trabalho se você já tem contato diário com essas pessoas.

Outras formas de criar redes de apoio com ajuda da internet são as velhas e ainda boas listas de e-mail. Você já teve a honra de conhecer o *We* (o serviço do *Riseup* de rede social), que, por si só, já é um meio. Mas saiba que o *Riseup* também tem listas seguras (bem mais seguras que de e-mails comerciais como as do *Google*). Se todo mundo já está junta e misturada no *Riseup*, por que não começar uma lista só de vocês? Tudo começa criando uma conta de lista **aqui**. Depois você ganha o superpoder de criar listas a partir do momento que entrar na sua conta. E aí convida geral.

6. O que mais posso fazer?
Quais são meus direitos?

Lembra quando a gente falou de leis lá nas **táticas de defesa #6** das redes sociais? Pois é, tudo aquilo se aplica na hora de denunciar uma má prestação de serviços. Mas lembre-se que todos estes *sites* possuem termos de serviço e supostamente nós aceitamos e concordamos com eles no momento em que criamos uma conta. Por isso, por mais dolorido que seja, leia (ou peça pra uma pessoa com mais paciência e entendimento jurídico) os termos de serviço antes de ir com toda sede ao pote praquela rede super legal que acabou de sair. E lembre-se também que, uma vez que você tenha solicitado para sair de um *site* e possivelmente deletado sua conta, esses termos não se aplicam mais a você. E caso você seja cobrada com relação a um uso não-solicitado, você tem todo o direito de reclamar esta cobrança.

CASO 2



Depois que fiquei sabendo que Google *lê meus e-mails não consigo mais mandar as mensagens que queria para as pessoas com quem estou me comunicando.*

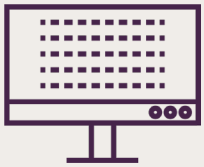
Estratégia 2

Não deixe que a página que caiu derrube você e seu coletivo.

O que vou proteger: minha privacidade, minhas informações pessoais, minhas mensagens privadas.

De quem vou proteger: adversários interessados em minhas informações pessoais ou informações sobre meu ativismo, *hackers* mal intencionados, empresas que comercializam meus dados, pessoas controladoras que querem acessar minhas informações privadas.

CONHECIMENTO É PODER



1. O que é criptografia?

A palavra é difícil, mas o conceito é simples quando a gente explica com carinho. :)

A criptografia, ou escrita secreta (sim, é assim que se traduz este nomezão), é um conceito que nos acompanha desde a antiguidade e já nasceu como uma necessidade de defesa. Imagina ter que mandar uma mensagem para uma pessoa aliada e ter um monte de inimiga no meio. Pesado. Mas e se você tiver uma linguagem que só você e as parceiras entendam? Tipo código, língua do P, aquelas estratégias de trocar a última letra com a primeira da próxima palavra. Sim, isto é tudo criptografia. Então, basicamente, criptografia é uma forma de codificar mensagens usando uma regra de base que só quem envia e recebe (ou outras pessoas que possuam esta regra, esta "chave") possam entender.

Óbvio que a criptografia da era da computação se tornou muito mais sofisticada graças aos algoritmos, ou seja, lógicas de programação que criam regras muito mais complexas que a língua do P ou a tal cifra de César. Mas, além de o sistema e o objetivo serem os mesmos, hoje contamos com vários métodos que tornam seu uso prático para qualquer tipo de comunicação. Mais do que isto: para proteger sua privacidade pessoal em arquivos do seu computador e celular.

2. Arquivos escondidos
no computador e celular.

Ao longo da Guia, falamos de um monte de criptografias de computador e talvez você nem tenha percebido. A seção de celulares está cheia de aplicativos legais de criptografia para esconder seus arquivos como o ***Secrecy,*** o ***KeepSafe***, o ***SecurePad*** e o ***Pic Lock***. Depois falamos sobre o *KeepassX* para guardar suas senhas e,sim, ele usa criptografia (por isto você precisa de uma senha-mestra, ela é a sua chave). E um monte de aplicativos de comunicação usam criptografia, até o *zap* (embora a criptografia dele não seja segura, afinal o servidor que tem as chaves é de uma empresa, então quem garante que alguém não tenha acesso a elas?).

Mas e se eu precisar manter aqueles arquivos importantíssimos seguros no meu computador? Aí eu posso usar o ***VeraCrypt*** . Ele faz a mesma coisa, ou melhor, ele é ainda mais sofisticado: ao invés de simplesmente camuflar seus arquivos, ele realmente cria um espaço totalmente criptografado no disco para que você coloque arquivos nele. E você pode inclusive mover esse espaço, que vai se parecer com um outro arquivo qualquer, pra outros computadores. Imagina que loko! Se você quiser um guia detalhado para *Windows* (e *Linux*, só mudar na página), pode seguir este **link aqui**.

3. Criptografia de email:
autodefesa de email.

O lance não era se comunicar de forma segura? Então! Hoje os principais aplicativos de *chat* usam criptografia até algum ponto, ou pra valer mesmo, como falamos do *Signal* e do *Wire* no capítulo passado. O que a gente chama de "pra valer" é a criptografia fim a fim, ou seja: ela não passa por nenhum servidor intermediário, é direto entre você e a outra pessoa, cada uma com sua chave. Isto já existe há muito tempo também para e-mails (e até protocolos de *chat* mais antigos) graças ao PGP (*Pretty Good Privacy*, ou como eu gosto de traduzir, privacidade boa mesmo). A gente ajuda você a entender mais sobre PGP lá no final, em "**Entenda bem, meu bem**", mas por hora é legal saber que a PGP é uma chave pessoal e intransferível que você pode, inclusive, certificar o quão confiável ela é sempre que as pessoas comprovarem que você é você. E aí, você pode trocar e-mails com outras pessoas que têm uma chave PGP de uma forma que você vai estar sempre segura da origem da mensagem a menos que alguém roube a chave e a senha da outra pessoa. Mas aí vocês já aprenderam como guardar essas coisas direto, né? Com essa lapada de dica que tem aqui...

Um guia bem explicado pra configurar seu e-mail e dar os seus primeiros passos no mundo da privacidade boa mesmo é **este aqui**.

4. Criptografia
de celular e de computador.

Então: já criptografou arquivo, e-mail, até as suas senhas. E o seu sistema do computador e do celular, como fica?

> *Oxe, mas precisa ainda?*

Precisa! Vamos explicar porquê: tudo que você faz no computador ou no celular é gravado, temporariamente ou permanentemente (em forma de arquivo). Mais exatamente nas memórias, a de acesso rápido (**RAM**), que é aquela que a gente ouve falar mais quando compra computador ou *notebook*, sabe? "*Notebook* xxt com 4GB de memória". O celular também tem, mas geralmente nas propagandas, quando falam "memória de 16GB", não é dessa que a gente tá falando (o negocinho é pequeno demais pra ter tanta). Aí a gente tá falando da memória de armazenamento (ROM), que no computador é o que a gente chama de HD, ou SSD, que inclusive é uma tecnologia parecida com a do armazenamento do celular, só que com bem mais espaço. Aí o que acontece: as informações que o sistema precisa pra ontem, ligeiro, ele fica guardando na memória **RAM**. E aí ele cria arquivos que guardam as configurações e um registro de como as coisas andam (isto é o que a gente chama de cache) dentro do HD ou armazenamento interno. Só que quando você desliga o celular ou o computador, a menos que você limpe, essas coisas continuam lá, e elas nem sempre são criptografadas. Na verdade, a maioria da informação no computador é texto puro (assim como a gente lê) ou binária e hexadecimal (sistemas de números que a máquina entende), mas que podem ser facilmente traduzidos por quem entende para texto. E a memória RAM costuma guardar o último estado dela mesmo depois de desligada, além do quê leva alguns segundos antes do computador e do celular desligarem para apagar os registros anteriores. Ou seja: na mão de quem sabe, isto é ouro.

Então, como faz? Todos os sistemas modernos (até o *Windows*, acredite) possuem meios de criptografar o sistema todo, no caso o **HD**. Essa técnica tem o nome de (adivinha?!): criptografia de disco inteiro. O único mais difícil de configurar é o *Linux* porque existem muitos tipos de sistemas de arquivos (que é o que realmente permite que o **HD** grave coisas), mas hoje tem vários sabores do *Linux* (as chamadas distribuições) que permitem que você faça a criptografia logo ao instalar, poupando muito trabalho (consulte o manual ou os fóruns do *Linux* que você usa; sempre tem informações de como fazer isso direitinho). Mas caso queira se tornar uma *nerd* de criptografia, tem o guia do ***Arch Linux*** (em espanhol, é o melhor que texiste atualmente) que é completíssimo e você pode usar em qualquer *Linux*.

No *MacOS* (antigo *OSX*), existe o ***FileVault*** que é uma ferramenta do sistema e a própria *Apple* (quem diria?!) tem um guia pra ajudar a habilitar. Aliás, o guia diz que o *FileVault* existe desde a versão 10.7, mas só com este nome. Já desde o 10.4 (*Tiger*) a criptografia funciona e o jeito de usar é o mesmo. No *Windows* a gente chama esta mesma coisa de *BitLocker* desde o *Windows 8*. **Este guia** ajuda a entender a coisa toda, e nem é tão difícil .

ENTENDA BEM
MEU BEM

Trolls: Na gíria da internet, designa uma pessoa cujo comportamento tende sistematicamente a desestabilizar uma discussão e a provocar e enfurecer as pessoas nela envolvidas.

Reconhecimento Facial: É uma técnica de biometria baseada nos traços do rosto das pessoas. A técnica feita através de computadores define traços únicos que devem ser mapeados em códigos, reconhecendo pessoas dos mais variados biotipos.

Criptografia: É um princípio e técnica pela qual a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Código aberto: é um modelo de desenvolvimento que promove um licenciamento livre para o design ou esquematização de um produto, e a redistribuição universal desse design ou esquema, dando a possibilidade para que qualquer um consulte, examine ou modifique o produto.

Biometria: São chamados de biometria os métodos de identificação pessoal através de características físicas únicas, como por exemplo a impressão digital, íris dos olhos e outros traços genéticos que individualizam uma pessoa.

VPN: Significa *Virtual Private Network*. Uma conexão de acesso privado e parcialmente anônima, onde você conecta a um servidor que permite a você utilizar outra rede através dele, escondendo assim o seu endereço IP e metadados de navegação do resto da rede.

DNS: Significa *Domain Name System*. É o sistema que permite que um servidor tenha um nome único reconhecido por toda a internet, gerenciando e direcionando o acesso feito aos endereços de internet.

***Nudes*:** A versão erótica das *selfies* (autorretratos feitos com celulares, usualmente). Ou seja, retratos íntimos tirados normalmente com celular, sejam parciais ou de corpo inteiro.

Metadados: São informações de identificação contidas em um arquivo, como tamanho, autora, programa ou equipamento utilizado para criá-lo etc. Quase sempre são transparentes para a pessoa que utiliza, mas podem ser pesquisados através de programas e usados para coletar informações específicas sobre ela.

Vingança pornô: A pornografia de vingança é uma modalidade que comumente expõe vídeos íntimos de mulheres, geralmente por seus ex-parceiros (ou parceiras), com a intenção de constrangê-las e assediá-las, como se fossem culpadas pela sua sexualidade. Estes vídeos também podem se tornar objetos de chantagem financeira e emocional, inclusive podendo causar transtornos profissionais e familiares na vida destas mulheres, resultado da visão patriarcal e misógina que a sociedade ainda possui sobre o sexo.

HD: Significa *Hard disk*, ou disco rígido. É a unidade de armazenamento interno do computador, onde seu sistema operacional, arquivos e programas ficam guardados.

RAM: Significa *Rapid Access Memory*. A memória que reserva informações que o sistema vai precisar acessar mais vezes enquanto executa aplicativos no seu computador ou celular. É acessada apenas pelos programas e pelo sistema, mas nada impede que um atacante escreva um vírus que acesse essa memória para descobrir dados pessoais enquanto seu dispositivo está ligado.

Sistema Operacional: Um conjunto de programas essenciais para que o computador funcione e possa ser operado por pessoas. Este sistema cria uma interface de usuário que permite que programas sejam instalados e as instruções da pessoa utilizadora sejam enviadas ao sistema físico ou hardware do seu computador ou celular.

Stalkear: Ato ou efeito de fuçar. Procurar informações sobre determinada pessoa nas redes sociais, sites e buscadores.

Voip: Significa *Voice Over IP*. É um protocolo de telefonia que permite que você faça chamadas telefônicas através do protocolo de internet.

Programas espiões: Também conhecidos como "*spywares*", são programas capazes de capturar comportamentos específicos da pessoa que utiliza o computador ou celular, como o que está sendo digitado ou clicado, ou armazenar registros de utilização.

Neutralidade da rede: A **neutralidade da rede** (ou neutralidade da Internet, ou princípio de neutralidade) significa que todas as informações que trafegam na rede devem ser tratadas da mesma forma, navegando à mesma velocidade. É esse princípio que garante o livre acesso a qualquer tipo de informação na rede.
Baculejo: O **baculejo** consiste na revista ou inspeção pessoal, por um policial diretamente no corpo da pessoa suspeita.

TFA (autenticação em dois fatores): Um modelo de autenticação onde você utiliza dois dispositivos para acessar um site ou aplicativo: um deles pessoal (como celular, *tablet* ou *token* eletrônico) que gera um código novo sempre que utilizado para ser inserido no outro dispositivo, após a senha. Por isso dois fatores: um é a sua senha, outro é o código pessoal.

***Token*:** Um dispositivo que serve exclusivamente para gerar códigos aleatórios seguros, pessoal e intransferível, para autenticações em dois fatores.

***Tor*:** *Tor* significa T*he Onion Router*, ou "*O Roteador Cebola*". O nome é dado porque esta rede é formada de múltiplas camadas que separam a pessoa utilizadora do seu destino na rede, usando pontos de conexão (*relays*) que passam a informação uns para os outros conhecendo só a si mesmos. No final, a sua conexão se torna completamente anônima para o servidor de destino. Para instalar o *TOR*, acessar **o link** e seguir os passos de instalação.

Navegação anônima: O modelo de navegação que permite que você não seja facilmente identificada, desde que tome os devidos cuidados essenciais, como não usar sites com tecnologias de script habilitadas (como *Flash* e *Javascript)* e utilize conexões seguras e anônimas. VPNs e o navegador da rede *Tor* (*Tor Browser*) são formas de se navegar anonimamente, cada uma com suas vantagens e desvantagens.

Endereço de internet ou IP: Os endereços de internet são obtidos de acordo com o protocolo de internet (IP ou *Internet Protocol*). Estes endereços são únicos para cada conexão de internet, sendo assim possível descobrir a localização geográfica e o provedor de acesso desse endereço, tornando cada dispositivo que acessa a internet identificável.

Cookies: São pequenos arquivos que permitem a um site que guarde informações de acesso ou autenticação no seu computador. Como estes arquivos ficam armazenados no seu computador ou celular, é possível que os sites utilizem para coletar informações essenciais da sua navegação na internet, como data, hora, navegador e sistemas utilizados, que são metadados muito preciosos.

Trackers: São muito parecidos com os cookies, mas estes particularmente permitem rastrear suas atividades de internet, como o acesso de um site para outro, publicidades que você clicou naquele site, e rotas de internet utilizadas para chegar até ele (inclusive podendo identificar de onde você conectou).

Cache: É um armazenamento temporário de dados que vão ser acessados constantemente durante uma sessão do sistema operacional ou do navegador e gravados no disco rígido ou na memória RAM. Podem ser lidos em tempo de execução ou serem coletados para verificação, no caso dos gravados em disco.

Servidor: Um computador com capacidades físicas e programas capazes de prover serviços na internet, como por exemplo hospedar um site ou um serviço de e-mails, entre muitos outros.

LINKS E BIBLIOGRAFIAS

- Como funciona o mercado brasileiro de ferramentas espiãs para celular
- Falha no iCloud é principal suspeita em vazamento de fotos nuas de celebridades
- Hacking Team é hackeada e tem seus documentos vazados
- Hackeando o Brasil
- Me, myself and I: Máscaras para nossas identidades conectadas
- Como manter o anonimato e contornar a censura na internet
- Entenda o que é a criptografia de ponta-a-ponta, utilizada pelo WhatsApp
- WhatsApp: dicas para proteger seus dados e conversas no mensageiro
- Como criptografar mensagens no WhatsApp
- Como funciona um chat secreto no Telegram
- Como ativar a verificação em duas etapas no Telegram e proteger a conta?

- **Como bloquear o Telegram com senha**
- **Como deixar o Instagram privado**
- **Como faço para iniciar uma conversa secreta no Messenger?**
- **Como bloqueio o Facebook de ouvir conversas?**
- **Saiba como 'esconder' sua lista de amigos no Facebook**
- **Manda nudes!**
- **Manda Prints!**
- **Neutralidade da Rede**
- **Busca Pessoal**

OAK FOUNDATION

FORDFOUNDATION

INTERNATIONAL WOMEN'S HEALTH COALITION

HEINRICH BÖLL STIFTUNG
A Fundação Política Verde

União Europeia

GLOBAL FUND FOR WOMEN