CELULARES & COMUNICAÇÕES: NOSSA BATALHA NO CAMPO VIRTUAL.

Enfrentando a violência contra nós, mulheres, no espaço virtual.

Celulares & comunicações: nossa batalha no campo virtual. Enfrentando a violência contra nós, mulheres, no espaço virtual.
Universidade Livre Feminista

Ficha Técnica

Coordenação geral: Cristina Lima e Jelena Dordevic

Textos: Fernanda Shirakawa, Fernanda Monteiro, Larissa Santiago e Débora Guaraná

Revisão e edição: Cristina Lima - MTb 31519

Revisão Técnica: Fernanda Shirakawa

Projeto gráfico e visual: Sarah Nicodemos

Conteúdo adaptado da Guia de Segurança Digital com contribuições de: Carla Jancz, Joana Varon, Maria Rita Casagrande, Priscilla Brito e Beth Ferreira.

Tiragem: impressa (500 exemplares)

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

Apoio: Oak Foundation, Ford Foundation e Fundo Global para Mulheres

A Universidade Livre Feminista é uma ação colaborativa compartilhada por uma Rede de Colaboradoras e apoiado pelo Centro Feminista de Estudos e Assessoria – CFEMEA, Cunhã Coletivo Feminista e SOS Corpo – Instituto Feminista para a Democracia.

www.feminismo.org.br

CELULARES & COMUNICAÇÕES:
NOSSA BATALHA NO CAMPO VIRTUAL

Enfrentando a violência contra nós, mulheres, no espaço virtual.

SEGURANÇA NA INTERNET:
NOSSA BATALHA NO CAMPO VIRTUAL

Nós, mulheres, estamos sujeitas a diversos tipos de violências em nosso cotidiano. A internet é apenas mais um espaço onde elas se manifestam.

Nos últimos anos, o movimento feminista tem ocupado a internet de diversas formas, especialmente as redes sociais. Além de nossa atuação nas ruas e em outros espaços nós, mulheres, estamos usando o espaço virtual para nossos encontros, discussões, mobilizações, organização e articulação. Isto está promovendo uma verdadeira transformação nos modos de existir do próprio movimento e da sua relação com a sociedade.

Ao mesmo tempo, têm se intensificado a criminalização e os ataques que sofremos no ambiente virtual. A cada dia, somos cada vez mais perseguidas em blogs, perfis nas redes sociais quando externamos nossos posicionamentos frente ao machismo, racismo, lesbo-transfobia e outras formas de violação de nossos direitos. Querem calar nossas vozes, derrubar nossos sites, blogs, nos humilhar e usar nossa imagem como objetos.

MUDANÇA DE COMPORTAMENTO

Para nos protegermos, precisamos mudar nosso comportamento sobre como estar na internet assim como na forma de utilizar ferramentas e dispositivos. Senhas, criptografia, proteção de dados, autocuidado e cuidado entre nós na rede, mais do que nunca, devem fazer parte de nosso dia a dia. Para nós, mulheres, ativistas, militantes, feministas, defensoras de direitos, segurança e proteção no espaço virtual precisam fazer parte de nossa ação política.

Longe de ser um material que tenha todas as informações sobre o tema, esta minicartilha pretende alertar mais mulheres sobre a importância e o lugar estratégico desta discussão. Até que ponto você está tomando os cuidados básicos para atuar na internet? Convidamos você para esta conversa.

CRIMINALIZAÇÃO E VIOLÊNCIA NO ESPAÇO VIRTUAL

A criminalização de movimentos sociais, organizações, coletivos e ativistas que defendem os direitos humanos no Brasil se intensificou a partir de junho de 2013, crescendo com o golpe institucional que destituiu Dilma Rousseff da Presidência da República e nas mobilizações "Fora Temer". Este processo tem sido facilitado e legitimado pela vigilância nos meios digitais e pelas leis resultantes das tentativas de controle das manifestações.

Nessa conjuntura, nós, mulheres, atuando em movimentos organizados ou mesmo como ativistas individuais no mundo digital, estamos sujeitas à essa vigilância e à violência que ameaçam o direito aos nossos corpos e vidas.

Por conta dessa investida 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 e movimentos, nossos corpos são alvo constante do assédio, do estupro, do racismo, da lesbofobia e da

transfobia, entre outras formas de discriminação e violência. Somos julgadas pela nossa aparência e comportamento. E se, nos espaços públicos, desde sempre travamos uma batalha em defesa de nossos corpos e nossos direitos, o mesmo acontece nos espaços 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?

Apesar da gradual ocupação desse espaço pelos 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?

CELULARES, INTERNET E SUAS CONEXÕES

Além de estarmos conectadas a computadores e tablets, os celulares têm sido poderosos instrumentos nas nossas mãos ativistas. Áudios, trocas, mensagens e todo tipo de informação tem circulado nesses nossos computadores de bolso, capazes de guardar e também espalhar um número infinito de informações sobre nós.

Esta cartilha é uma tentativa de conversamos sobre como podemos mudar alguns dos nossos comportamentos em relação a esse nosso companheiro diário, mostrando um pouco aqui como funciona a mágica e pensando em como podemos nos proteger e cuidar das nossas informações e dados.

QUAL O PREÇO DA NOSSA SEGURANÇA?

Na maioria das vezes em que usamos um serviço na internet, seja uma compra *online*, redes sociais, ou aplicativos de mensagens

instantâneas, estamos usando o serviço de uma empresa para enviar dados através de cabos.

É assim que a internet chega até nós:

Há um serviço que precisa ser contratado por um provedor (oferecido por empresas tais como a OI, NET, Velox, GVT). Elas instalam um roteador que emite um sinal wi-fi que nos conecta à rede mundial de computadores, a web. Caso a conexão seja feita pelo 3G do seu celular, o próprio telefone serve como roteador e tudo que você precisa é ativar um plano de internet na companhia telefônica.

Estes dispositivos fazem a ponte entre nós, os serviços disponíveis *online* e as pessoas com as quais nos conectamos através desses serviços. Cada serviço precisa de um servidor, ou seja, um computador físico, processando os dados que são recebidos e precisam ser enviados. O servidor do *Whatsapp*, por exemplo, é um

super computador que está localizado nos Estados Unidos. Ele é do mesmo dono do *Facebook*, do *Instagram* e de outros seis aplicativos pouco conhecidos no Brasil.

Quando mandamos uma mensagem para alguém que pode estar a poucos metros de distância de nós, os dados da mensagem vão ser enviados através de cabos físicos até o servidor do *Whatsapp* nos Estados Unidos, onde a mensagem é processada, armazenada e enviada ao destinatário pelo mesmo caminho percorrido.

Armazenada?! Sim, esse serviço é oferecido de maneira gratuita porque, em troca, você está oferecendo os seus dados. A operação é tão rápida que é difícil acreditar que uma mensagem percorre esse caminho todo e ainda é salva num computador que está localizado a milhares de quilômetros de distância. Ao final, o produto é você!

Outra coisa importante é cuidar dos acessos que podem acontecer nos pontos finais desse percurso, como nos celulares e computadores. Pessoas mal intencionadas podem instalar vírus ou quebrar suas senhas, por isto é importante cuidar da "saúde" dos seus equipamentos através de criptografia e senhas seguras.

TÁ, E A TROCO DE QUÊ ALGUÉM VAI ME ESPIONAR?

Isto depende, óbvio, de quem você é e de quem tem interesse na sua informação. Se você for uma ativista pode ser que sua militância incomode algumas pessoas e exista um interesse específico em quebrar a sua segurança. Mas infelizmente, de qualquer forma, todas nós estamos exposta a alguns interesses de espionagem.

Todos 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 fotos, áudios e vídeos. Ou seja, muita informação sobre você em tempo real.

Aí, vamos juntar umas informações: segundo os dados levantados pelo InternetLab, em abril de 2015, existiam cerca de 1.250 grampos Voips (telefone via internet como o Skype e ligação do *Whats*) e 15.000 grampos de telefone por mês no Brasil. Esses números demonstram que os grampos são feitos em massa e são mais do que só espiar "gente importante" por aí.

Além disso existem sites dedicados a vazar dados de câmeras públicas e privadas, informações pessoais de mulheres (!), dados de ativistas, pornografia de vingança (vazamento de fotos e vídeos íntimos sem consentimento), informações de crédito do banco, do cartão, da aposentadoria... Como dissemos antes, seus dados se convertem em dinheiro e poder, e tem muita gente de olho neles. E celulares não são bons com segredos.

Por isto quando nos comunicamos por telefone, os cuidados sempre são necessários. Em um mundo ideal, o melhor comportamento seria poder se comunicar por servidoras feministas autônomas com serviços, aplicativos de comunicação e redes sociais não-empresariais próprias, seguras, criptografadas fim a fim, que pudéssemos certificar a autenticidade das chaves sempre para garantir que nossos dados nunca fossem armazenados sem nosso consentimento.

MAS E NA PRESSA DO DIA-A-DIA, O QUE EU FAÇO SE NÃO TIVER ISSO TUDO?

A melhor prática é sempre procurar espalhar a mudança de cultura e comportamento. Se for possível ter conversas presenciais para assuntos muito importantes, ainda é o meio mais seguro e com verificação de segurança garantida. E se nas conversas virtuais você puder semear o uso do **Signal**, um aplicativo de mensagem seguro, gratuito, certificado por pessoas que acreditam em privacidade e livre para contribuições de qualquer pessoa, é uma excelente ideia. Ele usa criptografia fim a fim em todas suas comunicações, não é comercial e possui código aberto.

Outra opção de aplicativo seguro é o **Wire**, que além de criptografia fim a fim permite ligações de grupo criptografadas e troca de desenhinhos. Uma característica é que ele não requer um número de telefone para ser utilizado, e pode ser usado através de um aplicativo web ou desktop. Entretanto, sua segurança ao usar através do navegador também depende dele, então evite usar em computadores de outras

pessoas e cheque suas extensões e opções de privacidade. Além disso, o app para celular pode ser um pouco pesado para modelos mais antigos.

Mas por que não usar o *WhatsApp* mesmo? Bom, lembra que falamos dos interesses das empresas? O *WhatsApp* é do *Facebook* e essas duas empresas compartilham interesses e dados sobre você. Além disso, o *Whats* tem seus códigos fechados. Então apesar de dizerem que todas as mensagens são criptografadas, não temos como garantir.

E o ***Telegram***? O *Telegram* tem *chat* seguro apenas nas mensagens secretas e a criptografia utilizada nele possui falhas conhecidas. Apesar de não possuir criptografia, os *chats* do *Telegram* ainda são muito usados para grupos e redes de apoio. Se essa for a escolha, é necessário saber que esse *chats* não são protegidos e que as informações escritas dentro deles podem vazar, por isso tenha cautela.

ENTÃO EU PRECISO MESMO DE UMA SENHA?

Ter uma senha no celular é fundamental para não deixar tão fácil a vida de quem quer bisbilhotar suas informações. Escolha uma palavra ou frase fácil de lembrar e tente mesclar ela com número e caracteres especiais. A opção de **uma palavra é muito mais segura** que o Deslize ou que o PIN de números, pois esses têm poucas opções de combinações e podem ser visualizados através da gordura dos dedos na tela. Anote a senha em um papel e rasgue-a ou queime depois de decorada.

Após criar uma senha forte - prefira sempre senhas de letras e números, por serem mais difíceis de adivinhar - você cria a possibilidade de criptografar os dados do celular. Assim, caso você desligue seu celular, seus dados ficam inacessíveis sem acesso à senha. A maneira de habilitar a criptografia varia para Android, iOS (iPhone) e Windows Phone.

E O QUE É CRIPTOGRAFIA?

É uma técnica que transforma uma informação que seria fácil de entender ou acessar para qualquer pessoa em uma forma ilegível, de modo que possa ser conhecida apenas por pessoas que tenham recebido a chave "secreta" que converte de volta ao original (chamada de "chave criptográfica" ou "cifra"). Isto limita o número de pessoas que podem acessar essas informações e dificulta o acesso indesejado a elas.

Esta técnica pode ser usada tanto para proteger dados em comunicações de rede quanto arquivos e sua existência é anterior à computação. A "língua do P" é um exemplo de criptografia básica. Pjá psen psou pni pso? :)

COMO HABILITO CRIPTOGRAFIA NO CELULAR?

Caso você tenha um celular Android, é fácil de explicar: para criptografar seu celular, vá em **Configurações > Segurança > Criptografar telefone** (em algumas versões aparece como

Codificar - não espanta, é a mesma coisa). O telefone irá precisar da bateria do celular cheia, além de ser recomendado fazer *back up* (salvar na nuvem ou copiar noutro dispositivo) antes. E com um pouco de tempo, seu telefone fará o procedimento (máximo 30 minutos).

Para Windows Phone também: **Configurações > Sistema > Criptografia do Dispositivo** e então habilite a opção Ativado.

Para o iPhone, é importante dar uma lidinha nessas dicas para entender uns babados. Sabe como é a Apple né? Acesse: https://ssd.eff.org/pt-br/module/como-encriptar-seu-iphone.

ALGUÉM PODE ME OBRIGAR A REVELAR A SENHA DO MEU CELULAR?

Se esse alguém for um opressor que esteja acusando você de algo e queira saber a senha para "averiguar" seu telefone, saiba que, por lei, você não é obrigada a fornecer nada. 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.

Mas 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.

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 policial, o risco de você ter suas informações reveladas podem reduzir a zero. Pense nisso!

Para Android, tem também o ***Secrecy***: é um aplicativo de código aberto que usa um sistema de criptografia conhecido e testado. Ele é fácil de instalar e é gratuito. Para *Iphone* tente o ***Securepad*** e para *Windows Phone* o ***Pic Lock Ultimate***. Aprenda a usar cada um desses aplicativos na Guia de Segurança Digital.

Fonte: Guia Prática de Táticas e Estratégias para a Segurança Digital Feminista.
www.feminismo.org.br/guia

REALIZAÇÃO:

Universidade Livre Feminista

CFEMEA

SOS CORPO
Instituto Feminista para a Democracia

BLOGUEIRAS NEGRAS

maria [lab]

APOIO:

OAK FOUNDATION

GLOBAL FUND FOR WOMEN

FORDFOUNDATION