Image not found or type unknown

Cuidados em relação aos telefones celulares

Trabalhar junto às participantes a fim de trocarmos estratégicas e táticas de uso dos telefones celulares de forma mais segura considerando as situações e contextos em que vivem. É **altamente recomendado** que os participantes escolham um caminho de aprendizagem a percorrer, pois estes incluem actividades com diferentes níveis de profundidade que ajudam os participantes a obter mais conhecimentos sobre os temas abordados.

- Introdução e objetivos de aprendizagem
- Atividades de aprendizagem e caminhos de aprendizagem
- Dispositivos móveis, intimidades, acesso diferenciado por gênero e cuidados [atividade introdutória]
- Criando um cronograma de telefonia celular [atividade introdutória]
- Escalando o Himalaia [atividade introdutória]
- Coletando telefones celulares [atividade introdutória]
- Eu e meu telefone celular [atividade introdutória]
- Poderes das comunicações móveis – dispositivos, contas, serviços, estado, políticas [atividade de aprofundamento]
- O que é um telefone? Como as comunicações móveis funcionam? [atividade de aprofundamento]
- Debate: Documentação de violência [atividade de aprofundamento]
- Planejando comunicações móveis para ações/organização [atividade práticas]

- Faça Back-up! Bloqueie! Delete! a.k.a. Alguém pegou meu celular: Roubo, encarceramento, acidente, cruzar fronteiras. [atividade práticas]
- Discussão, interações + mão-na-massa: Escolhendo aplicativos móveis [atividade práticas]
- Usando dispositivos móveis para documentar violência: Planejamento e prática [atividade práticas]
- Reinicie sua segurança em aplicativos de paquera online [atividade práticas]
- Manda nudes, só que mais segura [atividade práticas]

Introdução e objetivos de aprendizagem


))#b!cld&'#df$sk84=)fgb*z"@gNTg#)
)jk&fjs#.udnf&//n;fgs
hv$%8/n,ifskY(99dd)))
s$sdfsfse#fsdgds&#
FRIENDS
COMMUNICATE
CUIDADOS CON

Neste módulo, trabalharemos junto às participantes a fim de trocarmos estratégicas e táticas de uso dos telefones celulares de forma mais segura considerando as situações e contextos em que vivem.

Este módulo oferece guias para facilitação de conversas sobre como ativistas pelos direitos das mulheres e pessoas transvestigêneres/cuir e pelos direitos reprodutivos usam as tecnologias de comunicação de forma distinta de acordo com suas narrativas de gênero. Nós iremos falar sobre como temos utilizado nossos celulares para comunicações pessoais e privadas, para comunicações públicas e dos movimentos que fazemos parte, e, também, sobre estratégias e ferramentas que estamos utilizando para administrarmos nossas comunicações móveis com mais segurança.

Este módulo inclui:

- atividades em grupo, investigando nosso uso de celulares e como isso está relacionado com nossas identidades de gênero e sexual;
- atividades ‘mão na massa’ para explorar e entender como nossos telefones celulares e comunicações móveis funcionam;
- atividades em grupo para trocas e práticas de estratégias e táticas de segurança dentro dos nossos contextos de vida;
- guias para facilitadoras sobre como construir pontes entre cuidados feminista e segurança digital.

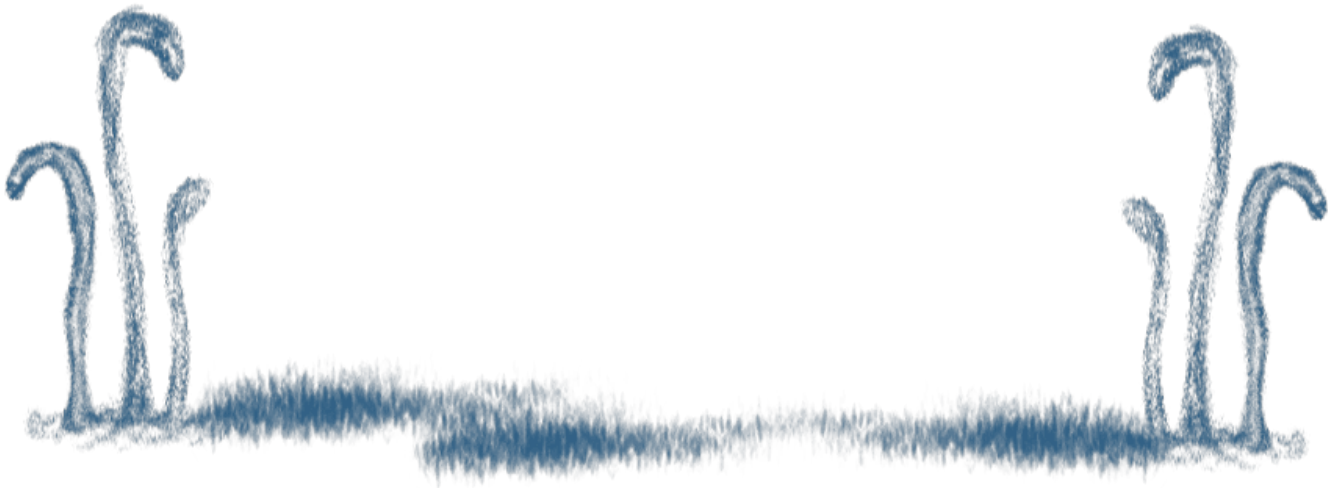
Seguem questões frequentes que temos ouvido e tentaremos encampar neste módulo:

- O que acontece se alguém mais tiver acesso ao meu telefone? Que informações estão no meu telefone? Como isso pode afetar a mim, meus colegas e o movimento do qual faço parte?
- Como descobrir se parceires, ex-companheires, membros da família, governo podem estar me vigiando?
- De que forma posso utilizar meu telefone com mais segurança?
- Como podemos utilizar nossos telefones para nos organizarmos?

Objetivos de aprendizagem

Ao final deste módulo, é esperado que as participantes tenham:

- um entendimento de como o acesso a comunicações móveis é diferenciado por gênero e é íntimo;
- um entendimento sobre cuidados em relação aos telefones celulares desde uma perspectiva de que eles são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;
- um entendimento dos conceitos básicos de como as comunicações via telefonia celular funcionam para que seus riscos possam ser melhor compreendidos;
- realizado trocas e praticado estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, colegas e nossos movimentos.



Atividades de aprendizagem e caminhos de aprendizagem

Esta página é essencial para o correcto uso e compreensão do Módulo. Seguir os Caminhos de Aprendizagem, com actividades de profundidade variável, permitirá ao participante obter uma melhor compreensão dos temas estudados.

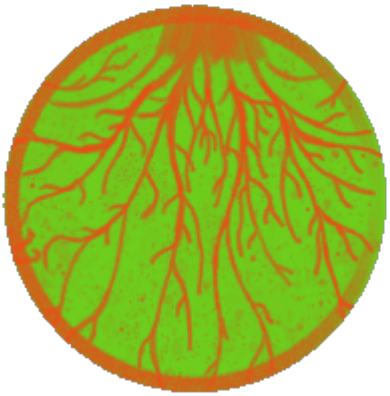
Atividades de aprendizagem

Atividades introdutórias



- Dispositivos móveis, intimidades, acesso diferenciado por gênero e cuidados
- Criando um cronograma de telefonia celular
- Escalando o Himalaia
- Coletando telefones celulares
- Eu e meu telefone celular

Atividades de aprofundamento



- Poderes das comunicações móveis – dispositivos, contas, serviços, estado, políticas
- O que é um telefone? Como as comunicações móveis funcionam?
- Debate: Documentação de violência

Atividades práticas



- Planejando comunicações móveis para ações/organização
- Faça Back-up! Bloqueie! Delete! a.k.a. Alguém pegou meu celular: roubo, encarceramento, acidente, cruzar fronteiras
- Discussão, interações + mão-na-massa: Escolhendo aplicativos móveis
- Usando dispositivos móveis para documentar violência: Planejamento e práticas
- Reinicie sua segurança em aplicativos de paquera online
- Manda nudes, mas com segurança

Atividades externas e baseadas em ferramentas

Onde os módulos incluem práticas e uso de ferramentas e softwares específicos, nós adicionamos links para recursos externos. Fazemos isso por algumas razões: os designs e recursos das ferramentas e os problemas de segurança mudam com frequência e, portanto, achamos melhor adicionar links aos recursos já com suas atualizações frequentes.

Caminhos de aprendizagem

Para facilitadoras que estiverem interessadas em alguma atividade específica, você pode usar somente uma atividade ou combinar algumas. Nós recomendamos começar com uma atividade inicial para abrir a discussão e as trocas entre as participantes sobre suas experiências com telefones celulares, e como gênero, sexualidade, raça, classe e capacitismo estão relacionados e impactam suas experiências.

Algumas recomendações específicas:

Para grupos que estejam considerando em usar o telefone celular para **documentação** de violência nós recomendamos a atividade de aprofundamento Debate: Documentação de Violência para abrir espaço para debater e discutir sobre desafios e oportunidades da documentação de violência e a atividade tática Usando dispositivos móveis para documentar violência: Planejamento e práticas.

Para grupos que queiram usar o **telefone celular para comunicações para ações e organização**, nós recomendamos as atividades táticas incluindo Planejando comunicações móveis para ações/organização e Faça Back-up! Bloqueie! Delete!.

Para participantes que usem o telefone celular para **namoro online e *sexting***, nós recomendamos a atividade inicial Coletando telefones celulares e as atividades táticas Reinicie sua segurança em aplicativos de paquera online e Manda nudes, mas com segurança.

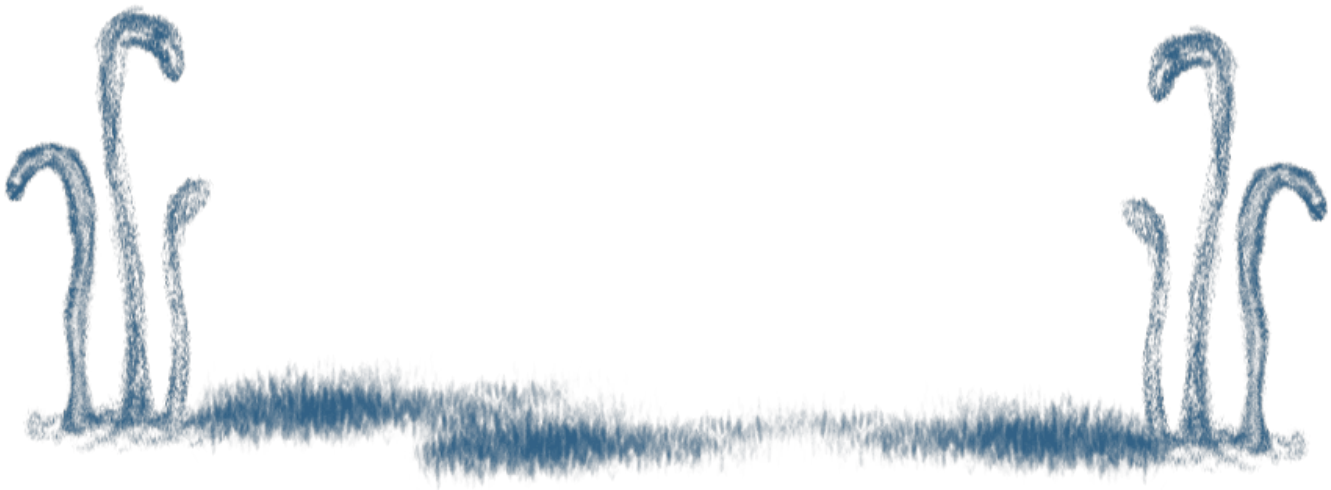
> **Nota da tradutora:** *Sexting* é uma forma de expressão da sexualidade onde pessoas trocam com consentimento palavras ou imagens de conteúdo erótico, sexual. Atualmente, pode ser exemplificado mais popularmente com os nudes, mas também em formatos anteriores como o telessexo e o chat erótico.

Nota especial para o treinamento segurança em telefonia celular

É muito raro que todas as participantes em um treinamento tenham o mesmo tipo de telefone celular. Logo, é uma boa ideia dividir em pequenos grupos quando em atividades práticas: usuáries de iPhone, diferentes versões de Android e/ou outros tipos específicos de usuáries.

Recursos | Links | Leitura adicional

- Guia Video for Change: https://video4change.org/resource-categories/ (em inglês)
- Guia Witness: https://portugues.witness.org/tutoriais /
- Security in a Box: https://securityinabox.org/pt/
- My Shadow: https://myshadow.org/pt [Os recursos para treinamentos não estão mais disponíveis, mas a guia de como controlar seus dados segue disponível na versão em inglês do site].
- EFF's Surveillance Self Defense: https://ssd.eff.org/pt-br



Dispositivos móveis, intimidades, acesso diferenciado por gênero e cuidados [atividade introdutória]

Nota da tradutora: o termo “intimidades” foi traduzido do original *Intimacy* – acreditamos que intimidades neste contexto se referem a formas de expressar afeto e sexualidade. Desde compartilhar *nudes* e mensagens de amor e carinho, como também, por exemplo, de poder se expressar enquanto LGBTQIA+ dentro de grupo e comunidades em redes sociais.

Nota da tradutora: o termo “acesso diferenciado por gênero” foi traduzido do original *Gendered Access* – entendemos como um acesso diferenciado por gênero, orientado a gênero. Acreditamos que este acesso de gênero se vê mais presente em culturas onde mulheres tem menos acesso a telefonia celular do que homens e/ou tem seu acesso cercado pelos mesmos (pais, irmãos, familiares, maridos).

Nota da tradutora: o termo “cuidados” foi traduzido do orginal *Safety* – ambas as palavras *safety e security* em português podem ser traduzidas como segurança, entretanto acreditamos que *safety* geralmente remete a uma segurança mais subjetiva e holística, uma sensação de segurança, por isso utilizamos a palavra cuidado.



Esta é uma **discussão introdutória** sobre as maneiras com as quais as participantes estão usando seus dispositivos móveis. Facilitadoras podem usar este exercício para introduzirem conceitos sobre o acesso diferenciado por gênero, para ressaltarem como nós manifestamos nossas identidades neste espaço das comunicações móveis e quais são suas possibilidades e seus riscos para as participantes.

Nós recomendamos fazer esta atividade no começo da oficina sobre cuidados nos dispositivos móveis.

Esta atividade apresenta 3 estágios:

- Troca entre pares
- Devolutiva entre o grupo
- Síntese de elementos comuns pela facilitadora

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento de como o acesso a comunicações móveis é diferenciado por gênero e é íntimo.

Para quem é esta atividade?

Esta atividade pode funcionar para qualquer pessoa que usa ou já usou um telefone celular.

Tempo estimado

Esta atividade requer cerca de 30 minutos.

Recursos necessários para esta atividade

- Quadro branco ou flip chart (se a facilitadora optar por escrever durante a devolutiva)

Dinâmica

Nossos telefones celulares são espaços de interações íntimas. Nós nos conectamos com as pessoas que amamos, amantes, amigues e compartilhamos ligações, mensagens, vídeos, conversas privadas e imagens. Ao fazer isto, nós vemos nossos telefones celulares como objetos íntimos, mas eles também fazem parte de um contexto maior, ligado aos provedores de serviço (companhias telefônicas), regulados por políticas governamentais, sujeitos a roubos/furtos e a serem acessados sem o nosso consentimento.

O acesso ao telefone celular varia de acordo com gênero e seu uso por pessoas mulheres/transvestigêneres/cuir representa um desafio ao poder – a autonomia e apropriação tecnológica destas pessoas com relação ao uso de dispositivos pode ser intimidador aos grupos dominantes; ao mesmo tempo que em outros contextos estes dispositivos podem usados para denunciarem abusos sofridos por essas pessoas.

Discussão entre pares - 15 minutos

Divididas em pares para facilitar trocas pessoais. Peça para uma partilhar primeiro enquanto a outra escuta. Em seguida, peça às parceiras que troquem os papéis de escuta e fala. Cada pessoa deve ter cerca de 5 a 7 minutos para falar. Isso dependerá também de quanto tempo se leva para os pares se formarem.

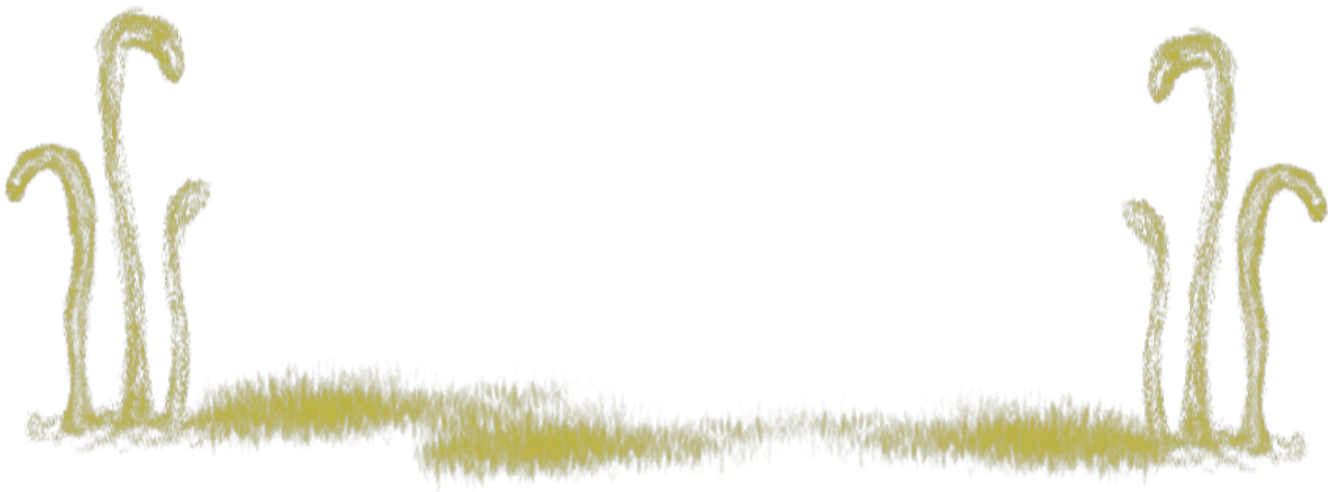
Questões

Escreva as perguntas em algum lugar visível para todas ou em papéis distribuídos para cada dupla.

- **Como você usa seu telefone celular? Quando você o utiliza?** *Se as pessoas ficarem bloqueadas, pergunte-as como elas usam para diferentes tipos de pessoas: amigues, familiares, colegas, estranhos*.
- **Como você usa o telefone celular para se organizar?**
- **Quando você se sente insegura usando seu telefone celular? O que você faz para lidar com esta situação?** *Encoraje as participantes a não discutir possibilidades de roubo/furto, estimule-as a compartilharem exemplos como parceires, amigos ou familiares espionando alguém; apreensões policiais, etc.*

Devolutiva entre o grupo - 15 minutos

A facilitadora toma notas e sintetiza. Existe alguma estratégia específica que você quer tratar, alguma situação ou possível cenário?



Criando um cronograma de telefonia celular [atividade introdutória]



Essa é uma atividade introdutória na qual as participantes irão partilhar suas histórias pessoais com telefones celulares e envolver as pessoas por meio de movimento corporal e contação de histórias. Espera-se que as participantes falem e ouçam sobre as suas atitudes em relação aos telefones celulares e compartilhem as formas pessoais e significavas com que estão usando e acessando seus telefones celulares.

Essa atividade é similar à Linha do tempo da Internet, que convida participantes a partilharem suas experiências com tecnologias móveis dentro de um cronograma. Através desta atividade, a(s) facilitadora(s) também podem se tornar mais familiarizadas com as experiências e relações que as participantes têm com seus telefones celulares.

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento de como o acesso a comunicações móveis é diferenciado por gênero e é íntimo.

Para quem é esta atividade?

Esta atividade pode funcionar para qualquer pessoa que usa ou já usou um telefone celular.

Tempo estimado

Esta atividade requer cerca de 30 minutos.

Recursos necessários para esta atividade

Etiquetas para marcar uma linha do tempo com datas em segmentos de 5 anos, 1990-2019. Podem ser números escritos no papel e colocados no chão (ex: 1990, 1995, 2000 etc.).

Dinâmica

Prepare um cronograma numa sala (como explicado acima). As participantes irão se deslocar e ficarão ao lado das datas respondendo a perguntas específicas que você fizer. Em um grupo grande, peça às participantes que se movam para uma data específica do cronograma respondendo as seguintes questões. Quando a linha de tempo for criada, pergunte quais serão as primeiras e as últimas datas. Se houver pessoas agrupadas em determinadas áreas do cronograma, pergunte em que período se encontram.

Dependendo do tamanho de seu grupo e de quanto tempo você terá, escolha 2 ou mais questões.

Peça a 1-2 participantes para responderem a questões específicas, por exemplo, “Como era naquela época?”.

Questões

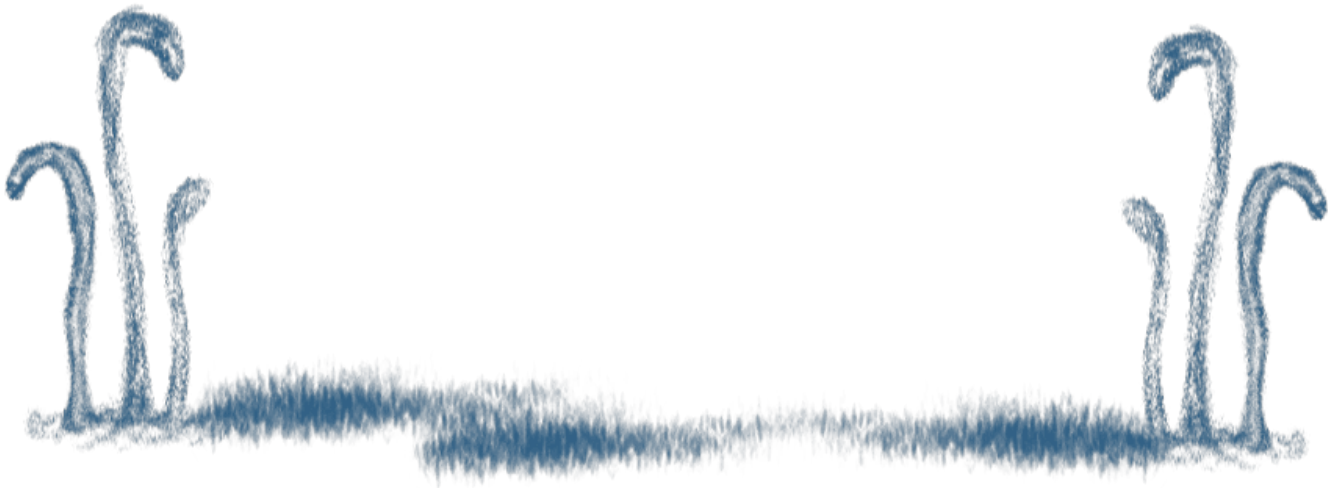
- **Quando foi a primeira vez que você teve um telefone?** Como foi? Você dividia o aparelho com mais alguém? Quantos anos você tinha? Para que ele era usado?
- **Quando você teve seu primeiro smartphone?** O que isso significa para você? Você compartilhava com alguém? Qual era seu app preferido? Por quê?

- **Quando você se conectou à internet pela primeira vez através do telefone?** Quais sites você acessou primeiro? Por quê?
- **Quando você “aposentou” um telefone pela primeira vez?** O que você guardou daquele telefone (i.e. Media tipo fotos, logs de textos, hardware)? Por quê?

Fechamento - 5-10 minutos

Pergunte para as participantes se elas têm comentários ou observações para compartilharem. Facilitadora, sintetize a atividade e conecte o que as pessoas compartilharam que tenha relação com acesso diferenciado por gênero e intimidades – considere o que as pessoas falaram sobre as atitudes que elas têm em relação aos seus telefones e às maneiras que elas gostam de usá-los.

> **Marcadores de diferença:** De que forma varia o acesso a telefonia celular e a privacidade entre as participantes baseada em seu gênero, sexualidade, raça, classe?



Escalando o Himalaia [atividade introdutória]



Esta é uma **atividade introdutória** para conscientizar as participantes sobre segurança nos telefones celulares e para facilitadoras e participantes avaliarem os tipos de medidas de segurança que as participantes estão tomando e as vulnerabilidades que podem ser as maiores prioridades a serem abordadas. Nós recomendamos fazer esta atividade logo no começo da oficina sobre segurança de dispositivos móveis.

Objetivos de aprendizagem aos quais esta atividade responde

- trocas e práticas de estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, nossas colegas e nossos movimentos;

Para quem é esta atividade?

Esta atividade pode funcionar para qualquer pessoa que usa ou já usou um telefone celular.

Tempo estimado

Esta atividade requer cerca de 30 minutos.

Dinâmica

Facilitadora pede às participantes que fiquem de pé e formem uma linha ombro com ombro. Pergunta questões sobre segurança de dispositivos móveis para as participantes. Instrui as participantes a darem um passo à frente caso a resposta para a pergunta seja SIM, e um passo atrás caso a resposta seja NÃO.

Exemplo de perguntas

- Você tem uma senha que bloqueia sua tela?
- Você usa aplicativos de bloqueio?
- Você tem um cartão SIM sem registro?
- Você tem um e-mail alternativo (que não seja a sua conta principal) para seu telefone celular?
- Você configurou os serviços de acesso remoto a seu celular? (ex.: Encontre meu telefone, "*Find my phone*")
- Os serviços de localização estão ativos no seu celular?
- Você tem back-up das mídias que estão no seu telefone celular (fotos, mensagens, vídeos etc.)?
- Você tem antivírus no seu telefone?

Fechamento - 5-10 minutos

Pergunte para as participantes se elas têm comentários ou observações para compartilharem. Facilitadora, sintetize a atividade e conecte a 'escalada' à agenda do dia ou série de sessões que vocês terão juntas.



Coletando telefones celulares [atividade introdutória]



Esta é uma **atividade introdutória** para sensibilizar as participantes sobre seus dispositivos móveis e outras pessoas quem tenham acesso a eles e a seus conteúdos.

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento de como o acesso a comunicações móveis é diferenciado por gênero e é íntimo;
- um entendimento sobre cuidados em relação aos telefones celulares desde uma perspectiva de que são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;

Para quem é esta atividade?

Esta atividade funciona particularmente bem no contexto pois as participantes da oficina vivenciam isso com frequência. Nós recomendamos este exercício caso as participantes estejam

experienciando apreensão de dispositivos e desejem discutir os impactos disso e suas respostas emocionais.

> **Observação sobre cuidados:** Recomendamos fazer isso com muito cuidado. Obtenha o consentimento claro e enfático das participantes. Esta atividade provavelmente funcionará melhor em um contexto em que você e as participantes já construíram uma confiança mútua profunda.

> **Uma nota sobre os caminhos de aprendizagem:** Esta é uma ótima atividade inicial para se preparar para discussões e atividades táticas sobre o preparo para situações de alto risco em que os telefones podem ser levados ou perdidos.

Tempo estimado

Esta atividade requer cerca de **30 minutos.**

Dinâmica

Atividade: Colete os telefones celulares das participantes e discuta – 15 minutos

Colete os telefones celulares das participantes bem no início, tendo o consentimento claro e empático das mesmas, mas sem explicar o porquê de estar coletando-os.

Discussão

Pergunte:

- Como você se sente em não ter seu telefone em suas mãos?
- Quais são seus sentimentos imediatos?

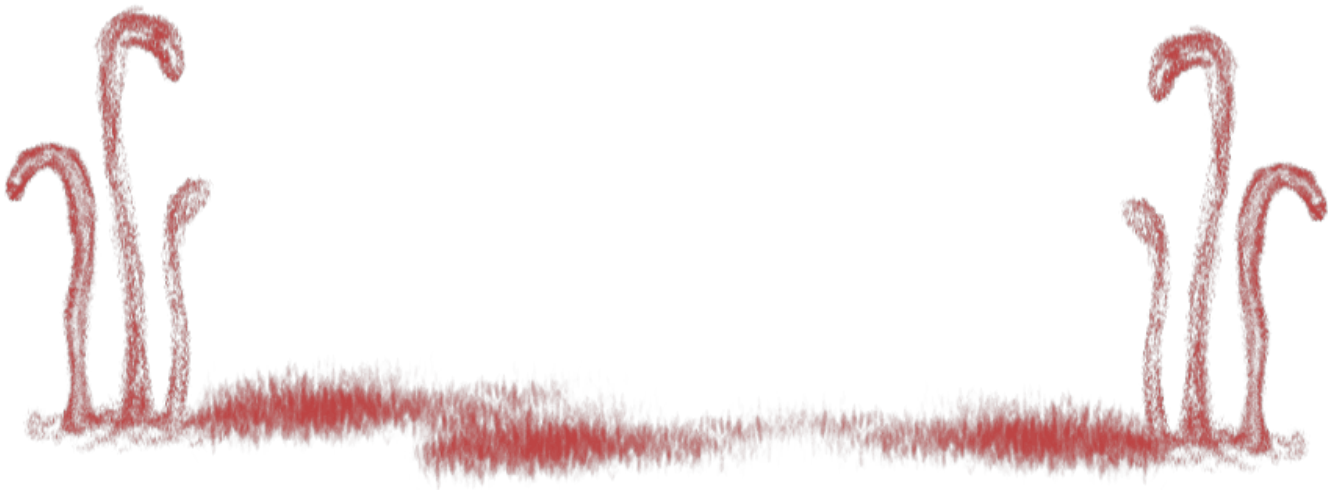
Atividade: Devolver telefones celulares e Fechamento - 5-10 minutos

Devolva os celulares que foram inicialmente coletados das participantes.

Discussão

Pergunte:

- Como se sentiu ao entregar o seu celular? Por quê?
- Como se sentiu ao ter de volta seu celular? Por quê?
- Existem momentos em que seu celular é tomado de você? Quem faz isso e em que situação?
- Como você se sente nesta situação? Por quê?
- Por que seu telefone é importante para você? Ao que o seu telefone dá acesso a você? Encoraje as participantes a serem específicas sobre como elas se relacionam com seus telefones celulares, ao que o telefone as conecta, e sua importância.



Eu e meu telefone celular [atividade introdutória]



Esta é uma **discussão introdutória.** Ela foi desenhada como uma atividade de curta duração, para facilitar a reflexão das participantes sobre como elas usam seus telefones celulares de formas íntimas e para que comecem a partilhar práticas e preocupações sobre vigilância e privacidade relacionadas a isso.

Nós recomendamos fazer esta atividade logo no começo da oficina sobre segurança de dispositivos móveis.

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento de como o acesso a comunicações móveis é diferenciado por gênero e é íntimo;

Para quem é esta atividade?

Esta atividade pode funcionar para qualquer pessoa que usa ou já usou um telefone celular.

Tempo estimado

Esta atividade requer cerca de 30 minutos.

Recursos necessários para esta atividade

- Quadro branco ou flip chart (se a facilitadora optar por escrever durante a devolutiva)

Dinâmica

Discussão em pares - 15 minutos

Divididas em pares para facilitar trocas pessoas. Peça para uma partilhar primeiro enquanto a outra escuta. Em seguida, peça às parceiras que troquem os papéis de escuta e fala. Cada pessoa deve ter cerca de 5 a 7 minutos para falar. Isso dependerá também de quanto tempo se leva para os pares se formarem.

Questão 1: Quais são as coisas mais pessoais e privadas que você faz usando seu telefone celular?

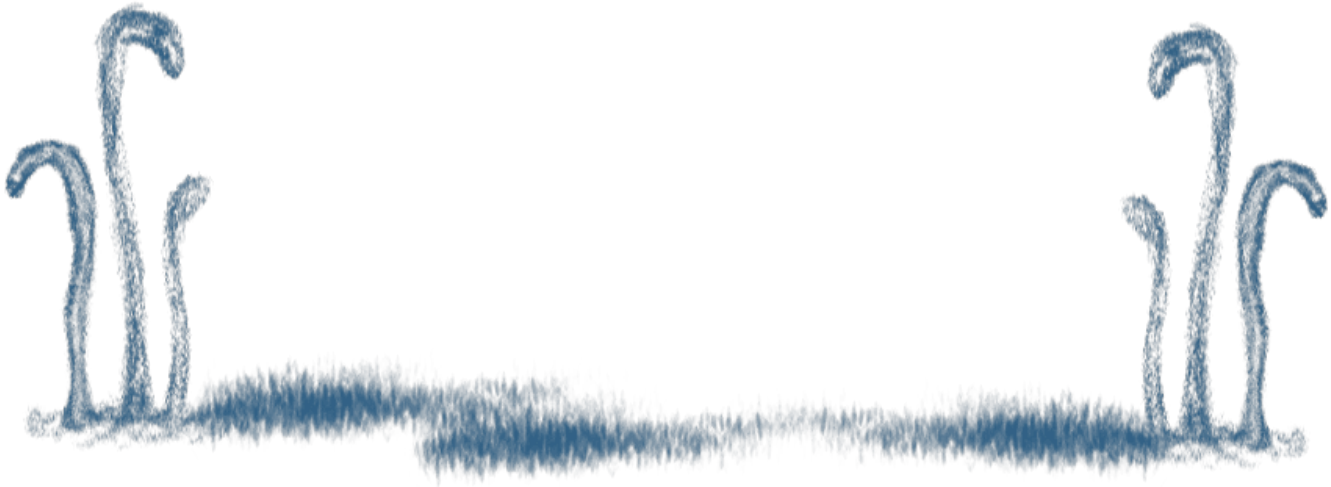
Questão 2: Como você cuida destas interações, mídia, experiências?

Facilitadora, dê um ou dois exemplos sobre o que partilhar em pares. Por exemplo, nudes que você tira para seu próprio prazer e para se expressar, sexting ou conversas íntimas que você está tendo com pessoas.

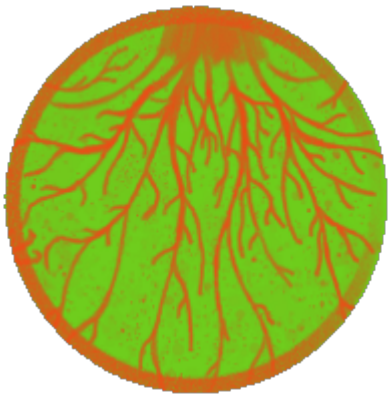
> **Marcadores de diferença:** De que forma varia o acesso a telefonia celular e a privacidade entre as participantes com base em seu gênero, sexualidade, raça, classe, capacidades?

Devolutiva do grupo todo - 15 minutos

A facilitadora toma notas e sintetiza. Peça para as pessoas compartilharem sobre o que elas falaram. Trace linhas em comum entre as conversas. De que forma as pessoas estão usando seus telefones e de que maneira estes usos são íntimos? Como as participantes partilharam que seu gênero está relacionado com o acesso que elas têm à telefonia celular, à sua privacidade? O que as pessoas estão fazendo para cuidarem de suas interações íntimas e suas mídias? Com o que as pessoas estão preocupadas e como elas estão relacionando privacidade e gênero, sexualidade, raça, classe, capacidades, idade, etc.?



Poderes das comunicações móveis – dispositivos, contas, serviços, estado, políticas [atividade de aprofundamento]



Esta é uma **atividade de mapeamento mental colaborativa.** Através de uma conversa guiada, o grupo irá discutir como elas se relacionam com seus aparelhos telefônicos, contas de serviços, provedores de serviços para telefonia móvel e um pouco sobre como as políticas corporativas e governamentais entram nesse jogo.

Nós recomendamos fazer esta atividade logo no começo da oficina sobre segurança de dispositivos móveis.

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento sobre cuidados em relação aos telefones celulares desde uma perspectiva de que são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;
- um entendimento dos conceitos básicos de como as comunicações via telefonia celular funcionam para que seus riscos possam ser melhor compreendidos;

Para quem é esta atividade?

Esta atividade pode funcionar para qualquer pessoa que usa ou já usou um telefone celular.

Tempo estimado

Esta atividade requer cerca de **45 minutos**, considerando como ela está escrita. Se você quiser agilizá-la, pode fazer menos perguntas às participantes e compartilhar um slide ou um exemplo do mapa mental.

Recursos necessários para esta atividade

- Folhas de *flip chart*
- canetas marcadoras

Dinâmica

Pergunte às participantes uma série de questões e faça um mapa mental com as respostas delas. O objetivo é tentar mapear as maneiras pelas quais as participantes se relacionam com seus telefones celulares. As participantes irão discutir sobre poderes, controle e agenciamentos das tecnologias móveis na medida em que discutem como se relacionam com seus **dispositivos móveis, contas de serviços, provedores de serviços para telefonia móvel e políticas corporativas e governamentais.**

Sugestões para preparação

- Familiarize-se com as operadoras locais;
- Familiarize-se com as conexões entre as operadoras locais e o governo (ex.: elas são governamentais?);
- Prepare alguns exemplos locais de maneiras em que ativistas pelos direitos das mulheres e pessoas transvestigênere/cuir estão usando seus telefones celulares, quais as relações de poder, como as corporações ou governos reagem/regulam, se aplicável;

Desenhe um mapa mental num lugar visível para que as pessoas possam se guiar enquanto você faz as perguntas.

- indique lugares onde as participantes falam de suas escolhas ou decisões (ex.: tipo de telefone, Android / Nokia; quem mais tem acesso ao telefone, como o escolheram; provedor de serviço; tipo de plano; quem tem acesso aos seus planos).

Exemplo de mapa mental. Clique para visualizá-lo maior. [em inglês]

mobile_screenshot.png
Image not found or type unknown

Questões para perguntar

Sobre dispositivos: Que tipo de telefone você usa? Como você conseguiu seu telefone? Você o divide com alguém? Como e com quem?

Sobre serviços móveis: Como você selecionou a operadora do seu telefone celular? Você compartilha um plano? Você gerencia seu plano? Se não, quem o faz? Você escolheu seu plano? Como?

Pergunte/discuta

A relação entre nós e nossa operadora de serviços de telefonia celular. Você assinou termos de serviço? O que você concordou quando assinou o contrato? Com o que a operadora concordou?

Nota para facilitadoras: Se você souber de preocupações específicas com as operadoras locais, tente encontrar e trazer exemplos de termos de serviço e/ou estudos de caso em que pessoas/clientes se envolveram com a operadora em torno da segurança.

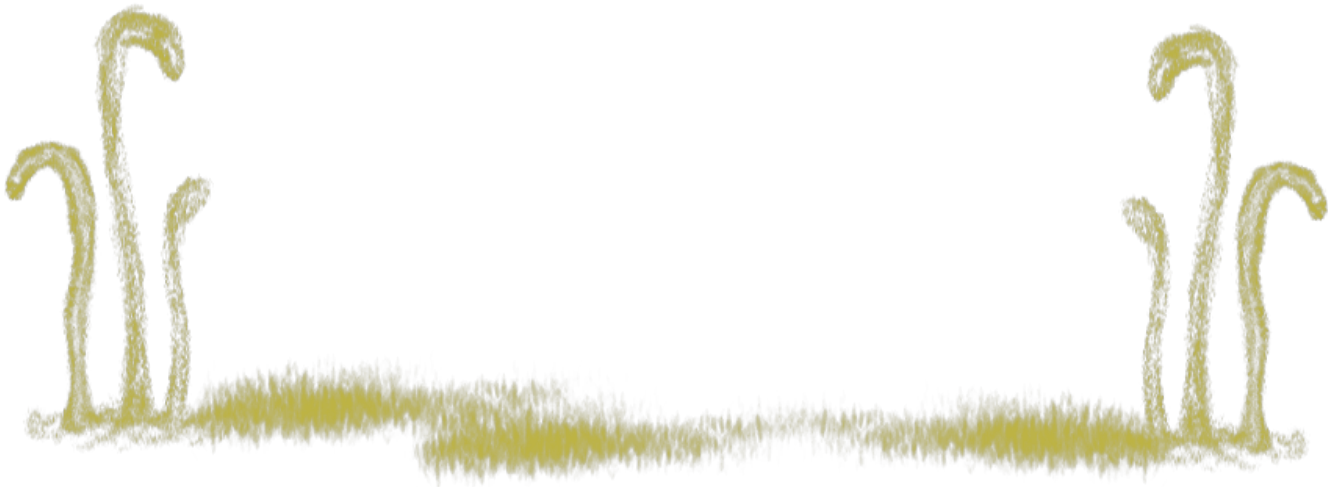
Pergunte/discuta

A relação entre as operadoras de celular e o governo. Estas são administrados pelo governo? São empresas internacionais, locais ou regionais?
Notas de facilitação: Você pode querer pesquisar com antecedência, regulamentações governamentais ou influências sobre o uso de dispositivos móveis. Houve algum desligamento de serviço recente? As participantes estão familiarizadas com o desligamento específico de linhas individuais? As forças de segurança apreendem dispositivos?

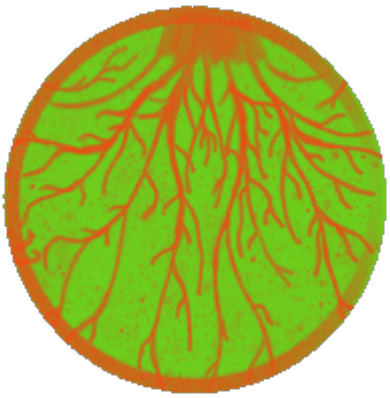
Recursos adicionais

Estudos de caso: como a *WRP continua usando esta atividade, adicione links relevantes para estudos de casos aqui*

- Uma página da Wikipedia listando operadoras de serviços móveis por país: https://en.wikipedia.org/wiki/List_of_telephone_operating_companies
- 101: Registro de cartões SIM (101: SIM Card Registration): https://privacyinternational.org/explainer/2654/101-sim-card-registration



O que é um telefone? Como as comunicações móveis funcionam? [atividade de aprofundamento]



O objetivo desta atividade é aprofundar o conhecimento de como as comunicações móveis funcionam para apoiar a capacidade do participante de avaliar e planejar os riscos das comunicações móveis. As facilitadoras devem incluí-la em qualquer oficina sobre comunicação móvel ou confirmar que todas as participantes já estão familiarizados com as informações desta atividade. É uma base para poder avaliar os riscos técnicos das comunicações móveis.

Esta atividade tem dois estágios:

- Dissecação mão-na-massa do telefone
- Entrada: dados das comunicações móveis e considerações de risco

Objetivos de aprendizagem aos quais esta atividade responde

- Compreender alguns conceitos básicos de como funcionam as comunicações móveis para nos informarmos sobre os potenciais impactos da utilização das comunicações móveis;

Para quem é esta atividade?

Esta atividade é para qualquer pessoa participando de uma oficina sobre telefonia celular.

Tempo estimado

Esta atividade requer cerca de **45 minutos.**

Recursos necessários para esta atividade

- alguns telefones celulares para abrir e investigar
- um quadro branco, slides ou apresentação

Dinâmica

Mencione ou discuta, dependendo do tempo disponível, que iremos falar sobre comunicações móveis – considerando dispositivos que são facilmente carregados na mão ou bolso e têm capacidades de comunicação desde chamadas de voz e SMS até internet e serviços de dados. Parte dessa sessão se aplica também a *tablets*.

Dentro dos nossos telefones - 5 minutos

Desmonte este telefone. Seu telefone é um pequeno computador. Todas peguem seus celulares e localizem:

- Partes que escutam e projetam sons: microfones, alto-falantes
- Partes que enxergam e mostram imagens: câmeras, telas
- Partes que mandam e recebem informações de outras fontes: GPS, Antena, Wi-fi
- Partes do computador, hardware: bateria, circuitos

- Memória: cartão SD, outra memória embutida no telefone
- *slot(s)* de Cartão SIM

Dispositivo e identidade SIM - 5 minutos

Seu telefone tem todas essas peças e alguns recursos de identificação, além da marca, modelo e sistema operacional, ele tem 2 nomes - um identificador de dispositivo e um identificador de cartão SIM. É importante saber sobre isso porque você pode ser identificado por qualquer um e seu telefone comunica essas informações com frequência, especialmente o IMSI.

- **IMEI** é o nome do seu dispositivo

International Mobile Equipment Identifier (IMEI):
https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- **IMSI** é o nome do seu cartão SIM

International Mobile Subscriber Identity (IMSI):
https://pt.wikipedia.org/wiki/International_mobile_subscriber_identity

Nossos telefones se comunicando - 35 minutos

Usamos nossos telefones para nos comunicarmos com as pessoas: SMS, Mensagens, Redes Sociais, Apps, Chamadas. Nossos celulares também comunicam informações sobre nossos telefones e sobre nós mesmas - não apenas nossas mensagens, mas metadados, nossa localização, etc., e isso pode ser vinculado a outras informações sobre nós, como nossas redes sociais, nossas redes de organização, nossos hábitos e locais de trabalho.

É bom estar ciente disso, principalmente para que possamos entender como o uso de nossos telefones celulares pode atuar como um dispositivo de rastreamento no momento e como um registro histórico de nossas atividades depois que elas acontecem.

1. Seu telefone é tagarela

Seu telefone está chamando diferentes tipos de redes e através de diferentes tipos de comunicação para anunciar que está próximo e para se conectar ou verificar se alguém deseja se conectar.

Operadoras de celular

As operadoras de celular têm torres e antenas com as quais seu telefone se comunica. Cada antena pode cobrir uma área específica. Seu telefone entra em contato com a(s) torre(s) que estiver mais próxima. Ele compartilha **pelo menos seu IMSI** para anunciar qual operadora de celular você está usando e seu número para que você possa receber mensagens, chamadas e comunicações em seu dispositivo. Cada vez que você está perto de uma torre, é como colocar um alfinete em uma linha do tempo mapeada onde você está. Você marca onde está, quando está lá e o que está fazendo naquele local em termos de uso do telefone.

GPS

Se o GPS estiver ativado, o telefone está se comunicando com satélites GPS, fazendo check-in de uma forma parecida, que é marcando com alfinetes em uma linha do tempo mapeada onde você está.

Wi-fi

Se o seu wi-fi estiver ligado, conforme você passa pelas redes wi-fi, seu dispositivo pode tentar se conectar a essas redes, deixando um registro com a rede wi-fi, e também gravar o nome da rede no seu telefone.

Bluetooth / NFC

Se estiverem ativados, outros dispositivos que usam Bluetooth e NFC podem se comunicar com seu dispositivo, tentar se conectar e compartilhar arquivos, etc.

Facilite a discussão: Quais coisas você precisa que estejam ligadas em quais momentos? Os registros de onde você está são um risco para você ou não?

2. Você é tagarela

Nós usamos nossos telefones para nos comunicarmos. Diferentes tipos de comunicação se mostram de forma diferente durante a comunicação e depois que as mensagens foram enviadas.

SMS

Mensagens de texto e metadados - na comunicação, uma vez armazenados no dispositivo e nas operadoras, são enviados em texto não criptografado. Uma analogia útil é que um SMS é como um cartão postal. Se alguém o interceptar, pode ler todo o conteúdo, bem como metadados (ex.: remetente, destinatário, hora, data).

MMS

Mensagens de mídia e metadados - na comunicação, podem ou não serem criptografadas, portanto, se alguém estiver tentando interceptar suas comunicações, varia se será possível vê-las. Depois de enviadas, você e os provedores e dispositivos móveis do seu destinatário têm um registro da mensagem e, portanto, a investigação sobre qualquer um deles pode revelar metadados (ex.: remetente, destinatário, hora, data) e conteúdo.

Chamadas

Conteúdo e metadados da chamada - da mesma forma - as chamadas devem ser criptografadas conforme estão em andamento, mas o seu provedor e o provedor do destinatário armazenam metadados sobre a chamada (por exemplo, remetente, destinatário, hora, data) e se o seu oponente tem acesso aos seus provedores, eles podem ter acesso para ouvir chamadas ou gravá-las.

> Para obter mais informações sobre aplicativos e aplicativos de mensagens, consulte: Discussão, interações + mão-na-massa: Escolhendo aplicativos móveis

Uma observação sobre a vigilância de Estado: de país para país, a vigilância de Estado varia. Em alguns lugares, os governos terão acesso a todos e quaisquer dados que as operadoras tenham - então, com eles, você deve considerar que todos os seus metadados e conteúdos de serviços não criptografados são acessíveis aos governos em tempo real e após o fato, se houver um investigação para esses registros.
Sua melhor defesa contra a vigilância é a criptografia de ponta-a-ponta.

3. Um telefone é um pequeno computador

Bug de software - um telefone é um computador e pode ser infectado com malware, assim como um desktop ou laptop. Indivíduos e governos usam software para bugar os dispositivos móveis de

outras pessoas. Este tipo de software geralmente usa partes do telefone para funcionar como um bug ou um dispositivo de rastreamento, ouvindo com o microfone ou enviando dados de localização.

4. A nuvem é um gabinete de arquivos

Alguns dados que meu telefone acessa não estão localizados no meu telefone, estão na nuvem. A "nuvem" é apenas um termo que significa "a internet" - dados que estão armazenados fisicamente em algum lugar com um dispositivo conectado à internet. Seus aplicativos podem estar acessando dados que estão na nuvem e não realmente em seu dispositivo.
Considerações: os meus dados estão criptografados no trânsito entre mim e o serviço? São criptografados quando armazenados pelo serviço? Sei de alguma ocasião em que oponentes tenham conseguido obter acesso a essas informações - quando, como?
Nota para a facilitadora: Enquanto você fala, os participantes podem fazer perguntas sobre partes dos telefones ou riscos associados aos métodos de comunicação mencionados. Tome o tempo para responder às perguntas. Se puder, mantenha uma lista contínua de questões e tópicos sobre os quais as pessoas pedem informações adicionais - uma lista contínua em um quadro branco bastará. Além disso, mantenha uma lista contínua de questões e tópicos que você não abordou nesta oficina específica, para que possa aborda-los mais tarde na oficina ou sugerir um acompanhamento após a oficina.

Recursos adicionais

- 7 maneiras de encontrar o número IMEI ou MEID do seu telefone (em inglês): http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- International Mobile Equipment Identifier (IMEI) (em inglês): https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
- International Mobile Subscriber Identity (IMSI)(em inglês): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

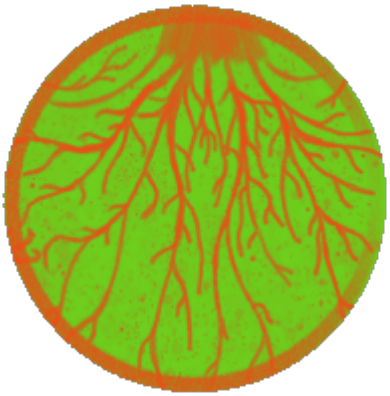
O site My Shadow do Tactical Tech tem várias guias de treinamento excelentes para facilitar o aprendizado sobre tecnologia móvel.

- My Shadow downloadable materials: https://myshadow.org/materials (em inglês)

- My Shadow website: https://myshadow.org/pt



Debate: Documentação de violência [atividade de aprofundamento]



Esta é uma atividade de **discussão aprofundada** para facilitar a discussão sobre o uso de celulares para documentar a violência e como isso se relaciona com a perpetuação da violência. Este exercício pode ser usado para discutir casos específicos de mídias ativistas focadas na redução da violência, quando estes mesmos canais e mídias acabaram sendo utilizados para veicular e assim, muitas vezes, perpetuar a violência. As participantes compartilharão exemplos de como estão usando celulares para documentar a violência e se envolverão em debates sobre os impactos do compartilhamento de documentação da violência online.

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento sobre cuidados em relação aos telefones celulares desde uma perspectiva de que são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;

Para quem é esta atividade?

Grupos que já utilizam ou estão pensando em utilizar telefones celular para documentar violência.

Tempo estimado

Esta atividade requer cerca de **60 minutos.**

Recursos necessários para esta atividade

- Estudos de casos impressos ou links

Dinâmica

Plenária - 10 minutos

Peça às participantes para compartilharem maneiras com as quais elas usam seus telefones celulares para documentarem violência.

> **Nota de cuidados:** As pessoas podem compartilhar incidentes que ativam gatilhos para si mesmas e para outras pessoas na sala. Ao pedir que as pessoas compartilhem, ao pedir exemplos, reconheça quaisquer acordos e normas de seu espaço quanto a falar sobre violência. Você pode dizer reconhecer que o exercício discutirá atos de violência e que as pessoas que estão compartilhando são convidadas a compartilhar e cuidar de si mesmas, ou seja, a compartilhar de uma forma que não ultrapasse sua própria capacidade. Você pode pedir às pessoas que se cuidem e caso sintam gatilhos, que elas parem de compartilhar e/ou cuidem-se como precisarem.

Pergunte:

- Quais são os exemplos de documentação de violência e partilha desta documentação que tiveram um impacto positivo em seu trabalho, *advocacy*, para suas comunidades?

- O que você estava documentando?
- O que aconteceu?
- Como você compartilhou?
- Com quem você compartilhou e como você escolheu estas pessoas?
- Qual foi a resposta obtida?

Facilitadoras poderão preparar exemplos de movimentos locais e recentes usando celulares para documentar a violência e pedir às participantes que compartilhem exemplos de como estão usando celulares para documentar a violência ou para compartilhar documentação. Os exemplos podem incluir: documentar a violência do Estado, encaminhar vídeos de atos violentos, violência ao vivo, as implicações de possuir a posse desse tipo de mídia.
Alguns exemplos estão vinculados na seção "**Recursos adicionais**" abaixo. Você pode escolher usá-los para estudos de caso em pequenos grupos ou selecionar exemplos mais atuais ou apropriados para suas participantes.

Explique que esta atividade visa facilitar o espaço de discussão e debate em torno deste uso.

Pequenos grupos - estudos de caso - 20 minutos

Dê a cada pequeno grupo um estudo de caso para ler e discutir. Você pode encontrar estudos de caso abaixo - escolha e edite cenários de caso, postagens de blog e artigos de notícias, ou escolha ou escreva exemplos que sejam mais relevantes para suas participantes.

- Qual é o exemplo?
- Quais são os argumentos a favor do uso de telefones celulares para documentar violência neste caso?
- Quais são os argumentos contra o uso de telefones celulares para documentar violência neste caso?
- Quais são algumas maneiras de reduzir os impactos negativos desse tipo de vídeo que documenta a violência?

Cenários

Esses cenários são exemplos de uma maneira de se escrever cenários para as participantes da oficina. Ao escrever mais de 1, você pode levantar várias questões que sabe que os participantes vão querer discutir. Os exemplos aqui são projetados para iniciar conversas sobre vincular documentação ao movimento, consentimento, impacto e perpetuação da violência.

Cenário 1

Sua comunidade tem enfrentado violência e assédio. Você e outras se organizaram para documentar atos específicos e compartilhar alguns deles em plataformas de mídia social com legendas e texto para explicar os incidentes e a violência em curso. Você pode ligá-los a recursos, incluindo uma lista de demandas de sua comunidade e recursos de apoio para pessoas que estão sofrendo violência semelhante.

Cenário 2

Você testemunha um ato de violência na rua e começa a transmiti-lo ao vivo para seu canal de mídia social, onde tem milhares de seguidores. Você não conhece as pessoas que está filmando e não conhece o contexto.

Cenário 3

Você e sua comunidade têm transmitido ao vivo as imagens das manifestações para mostrar o poder das manifestações e documentar incidentes de violência e danos causados aos manifestantes. Você fica ciente de que a filmagem está sendo usada pela polícia local e por grupos de oposição para atingir os manifestantes, e editada em conjunto para criar uma mídia de oposição sobre os manifestantes que também está sendo compartilhada nas redes sociais.

Plenária – devolutiva - 30 minutos

A devolutiva em grupo é uma oportunidade para cada grupo compartilhar seu caso de estudo e ter uma discussão com o grupo todo sobre os atuais desafios em se documentar violência e compartilhá-la online. Permita um tempo amplo para os grupos partilharem e para que possa haver engajamento.

- Qual é o exemplo?
- Quais foram os argumentos a favor e contra do uso de telefones celulares para documentar violência que surgiram sobre este caso?

- O que isso suscita para as outras? Você encontra esse problema? Como você está pensando nisso? Como você está traçando estratégias para obter o melhor impacto possível e como está reduzindo a probabilidade ou os impactos negativos?

Facilitadoras, à medida que os participantes compartilham, aponte os temas comuns. Quais são as principais preocupações das suas participantes em seus trabalhos - alguns problemas que podem surgir e sobre os quais você pode facilitar as sessões mais especificamente, podem incluir questões táticas de como documentar, armazenar, compartilhar; questões de verificação de mídia, falsificações profundas (*deep fakes*); uso da mídia para incitar violência e a possibilidade de compartilhar a documentação da violência como perpetuadora da violência e do dano.

Recursos adicionais

Estudos de caso e postagens em blogs sobre os impactos da documentação da violência

Exemplos de como as pessoas estão usando celulares para se organizarem - sugerimos reunir exemplos locais ou atuais relevantes de como as organizadoras estão usando celulares e pedir às participantes e anfitriãs exemplos durante a preparação da oficina.

- Documentação de abusos de trabalhadores migrantes (em inglês)
    - Centre for Migrant Advocacy´s OFW-SOS

Estudo de caso: transmissão ao vivo de atos violentos: os desafios éticos da transmissão ao vivo pela Internet, Irie Crenshaw e Justin Pehoski (Live streaming violent acts Case Study: The Ethical Challenges of Live Internet Broadcasting)

https://mediaengagement.org/research/matters-of-facebook-live-or-death/

- Australia (em inglês)

O mundo está se voltando contra a transmissão ao vivo. Após o tiroteio em Christchurch, a Austrália está liderando a investida contra vídeo bruto e não filtrado, Casey Newton, 4 de abril de 2019 (The world is turning against live streaming, In the aftermath of the Christchurch shooting, Australia is leading the charge against raw, unfiltered video) https://www.theverge.com/interface/2019/4/4/18294951/australia-live-streaming-law-facebook-twitter-periscope

- Exemplos do Brasil (em inglês)

Despacho do Brasil: Se for morto pela polícia, será culpado por padrão... a menos que haja vídeo?, Priscila Neri (Dispatch from Brazil: If killed by police, guilty by default... unless there's video?) https://lab.witness.org/dispatch-from-brazil-if-killed-by-police-guilty-by-default-unless-theres-video/

- WhatsApp e violência na Índia (em inglês)

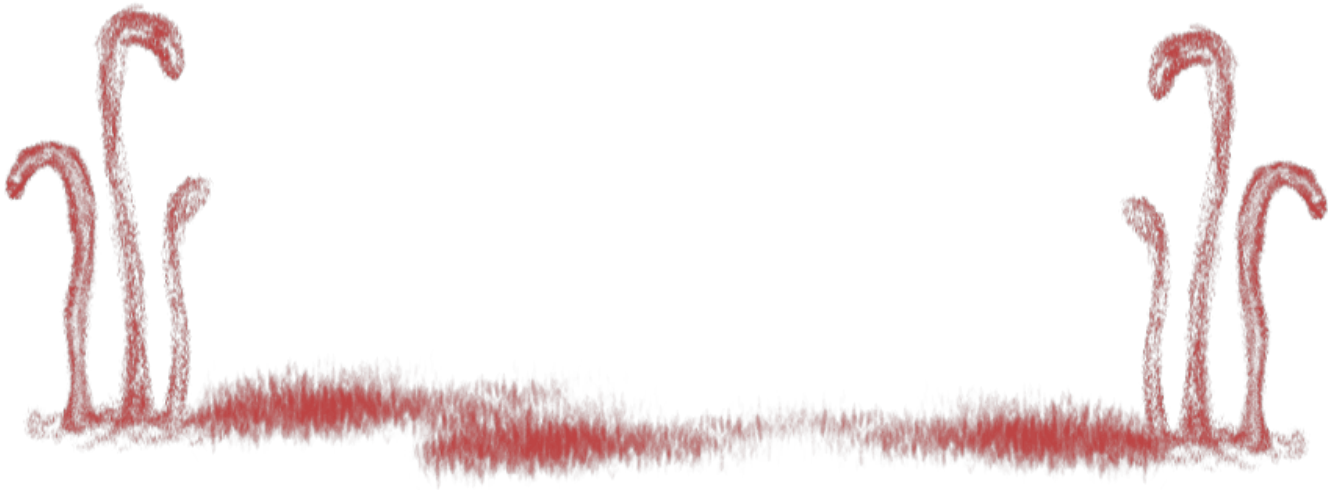
O WhatsApp limitará drasticamente o encaminhamento em todo o mundo para impedir a disseminação de notícias falsas, após a violência na Índia e em Mianmar, Kurt Wagner, 19 de julho de 2018 (WhatsApp will drastically limit forwarding across the globe to stop the spread of fake news, following violence in India and Myanmar) https://www.vox.com/2018/7/19/17594156/whatsapp-limit-forwarding-fake-news-violence-india-myanmar

- USA examples (em inglês)

Momento de vídeo viral da C-SPAN, Hadas Gold, 22/06/2016 (C-SPAN's viral video moment)

https://www.politico.com/story/2016/06/cspan-house-sitin-democrats-224696

Membros do Congresso dos EUA transmitem ao vivo uma manifestação exigindo uma votação sobre a legislação de controle de armas. (US Congress members livestream a sit-in demanding a vote on gun-control legislation.)



Planejando comunicações móveis para ações/organização [atividade práticas]



Abaixo apontamos considerações de orientação para grupos que estão se organizando e participando de ações utilizando aplicativos de mensagens. Usando esta guia, você pode facilitar discussões para ajudar grupos a refletirem sobre como são suas formas de comunicação e fazer o design de protocolos de gerenciamento de grupos, mensagens e de dispositivos que atendam às necessidades de segurança dessa comunicação.

Esta atividade conta com 3 estágios:

- Mapeamento de comunicações e avaliação de riscos
- Planejamento: fazer um design de grupos e configurações
- Instalação de Aplicativos (opcional)
- Implementação (opcional)

Se os grupos não tiverem escolhido ainda qual aplicativo de mensagens querem usar, você pode fazer a atividade Discussão, interações + mão-na-massa: Escolhendo aplicativos móveis

Objetivos de aprendizagem aos quais esta atividade responde

- trocar e praticar estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, nossas colegas e nossos movimentos;

Para quem é esta atividade?

Esta atividade é para participantes com variados níveis de experiência em usar telefones celulares. Se entre as participantes tiver pessoas que serão administradoras dos grupos de mensagens, planeje implementar os projetos na própria oficina.

Tempo estimado

Esta atividade requer cerca de **60 minutos** para o mapeamento e projeto e até 3 horas se você irá instalar os aplicativos de mensagens, mapear, projetar e implementar o projeto.

Recursos necessários para esta atividade

- Papel para as pessoas fazerem o design de seus projetos e completarem o mapeamento

Dinâmica

Mapeamento de comunicações e avaliação de riscos

Consideração: Privacidade

Considere que você pode ter diferentes tipos de mensagens para comunicar por meio do Signal e que algumas mensagens são mais públicas do que outras. Mapeie os tipos de comunicação que você faz e faça o design de grupos de acordo com suas considerações de privacidade.
Que tipo de comunicação você está fazendo e quais considerações você tem sobre quem tem acesso à comunicação? Sugira que as participantes considerem esses diferentes grupos. Pergunte se elas têm mais tipos de informações - por exemplo, há informações que apenas 2 pessoas devem saber, que apenas uma pessoa deve saber e documentar e não compartilhar?

QUEM	EXEMPLO DE COMUNICAÇÃO

1 precisa ser mantida entre um grupo bem pequeno de pessoas que se conhecem entre si	*localização das principais organizadoras*

2 é vital que as voluntárias saibam ou que pequenos grupos se coordenem	*mudanças na localização da multidão*

3 pode ser compartilhada abertamente	*hora de início da manifestação, grupos que endossam esta ação publicamente*

Planejamento: design de grupos e configurações

Trabalhe com as participantes para fazer o design de grupos que correspondam aos diferentes tipos de comunicação.

Sugestões de orientação sobre o design do grupo: Sugerimos começar com estas questões de design. Incluímos sugestões de exemplo para o gerenciamento de grupos e configurações para alguns tipos mais comuns de grupos. Pergunte às participantes o que vai funcionar e o que não vai para elas, facilite a modificação dos designs dos grupos para melhorar as partes que não funcionam.

Membros

- QUEM – Quem pode entrar neste grupo?
- COMO – Como as pessoas entram neste grupo? Qual o procedimento? Elas precisam ser avaliadas, apresentadas, são inseridas automaticamente, ou se inscrevem?
- RECONHECIMENTO - Como o grupo reconhece quando uma pessoa se junta? Por que você gostaria que o grupo fizesse isso ou não?

- ACORDOS – O que você faz se alguém entrar sem seguir os procedimentos?
- INFORMAÇÕES PESSOAIS - com o serviço de mensagens que você está usando, membros do grupo podem ver os números de telefone de outras do grupo? Nesse caso, para quem precisa que seu número não seja conhecido como parte da organização, não deve se juntar a nenhum grupo grande em que as outras pessoas ainda não saibam seu número e que a pessoa faz esse trabalho.

Saiba com quem você está falando - VERIFICAÇÃO

Para cada tipo de comunicação, como você irá verificar com quem você está de fato falando?

- CARA-A-CARA - você exigirá que algum membro do grupo encontre o resto do grupo cara a cara para ingressar? Uma pessoa pode simplesmente ser adicionada e certificada por um membro do grupo?
- Nºs DE SEGURANÇA - VERIFIQUE se suas mensagens estão indo para os dispositivos corretos. Se você estiver usando Signal ou WhatsApp, VERIFIQUE OS NÚMEROS DE SEGURANÇA
- PALAVRAS DE SEGURANÇA - VERIFIQUE se suas chamadas estão indo para os dispositivos corretos. Se você estiver usando o Signal para chamadas, FALE AS PALAVRAS DE SEGURANÇA com a pessoa que deseja falar. Se você estiver usando outro aplicativo de chamadas, pense se quer ter uma maneira de fazer check-in no início de uma chamada para verificar se a pessoa é quem você pretendia e está falando livremente.

Segurança de mensagens - configurações

Discuta, com base na sensibilidade das informações que você está comunicando, que tipo de acordos você deseja fazer sobre como as pessoas estão usando as configurações de mensagens. Por exemplo:

- DELETAR Mensagens - Por quanto tempo os membros do grupo devem manter logs de bate-papo em seus dispositivos?
- Mensagens EFÊMERAS - Em um chat do Signal, você pode definir quanto tempo as mensagens permanecerão antes de serem excluídas automaticamente. Você quer usar este recurso? Como e por quê?
- OCULTAR mensagens na tela inicial - Configure os aplicativos de mensagens para não serem visualizados na tela inicial, de modo que, se você perder o controle do dispositivo,

as pessoas não poderão ver o conteúdo da mensagem na tela inicial.
- CÓDIGOS - Para informações extremamente confidenciais, sugerimos estabelecer palavras-código antes de planejar e agir. Por exemplo, você pode substituir as palavras "Estamos prontos para a festa do chá" em vez de "Prontos para o protesto!"

Modelos de design para grupos

1. Pequenos grupos altamente verificados para informações confidenciais

> Consideração/risco: que as pessoas entrarão em grupos desconhecidos e que não sabem se as informações lá veiculadas podem ser publicizadas ou não.

- Se você tiver informações confidenciais que precisam ser compartilhadas apenas entre um conjunto de pessoas conhecidas;
- Grupo muito pequeno, 8 ou menos, todos se conhecem e se encontraram cara a cara;
- Adicione pessoas apenas quando estiver cara a cara;
- VERIFICAR Identidade (no Sinal, verificar Números de Segurança) pessoalmente;
- Se o número de segurança de alguém mudar, verifique novamente pessoalmente;
- Não diga mais do que o necessário, não corra riscos desnecessários;
- DELETE

2. Células - grupos de trabalho reduzidos

> Consideração/risco: Que as pessoas se juntem ao grupo e enviem informações que não sejam úteis ou intencionalmente incorretas.

- Desta maneira, diminui o risco de indivíduos enviarem spam para um grande grupo e torná-lo inutilizável e cheio de ruídos;
- Grupo de 2 a 20 pessoas, o que for necessário para se manter o número de mensagens baixo e ter um número gerenciável de células no Signal;
- Um grande grupo pode ter várias células para manter a comunicação gerenciável e relevante;

- As células são conectadas umas às outras para que as informações possam fluir entre elas. Você pode considerar ter uma pessoa-chave em cada célula para que elas possam enviar informações que todos precisam ter.

3. Grupo aberto, informação pública

Considere as informações neste canal como informações públicas em tempo real. Embora as informações de qualquer um dos outros grupos possam vazar ou ser compartilhadas fora do grupo, este é um grupo que você automaticamente considera público.

- Se você tiver alguma informação para compartilhar que possa ser tornada pública, use este modelo!

Segurança do dispositivo

Se o seu dispositivo for levado, evite que outras pessoas finjam ser você e leiam suas informações, como mensagens de sinal, catálogo de contatos, e-mail, etc. Para orientações de facilitação mais detalhadas sobre segurança de dispositivos, consulte a atividade: Faça Back-up! Bloqueie! Delete! a.k.a. Alguém pegou meu celular: Roubo, encarceramento, acidente, cruzar fronteiras.

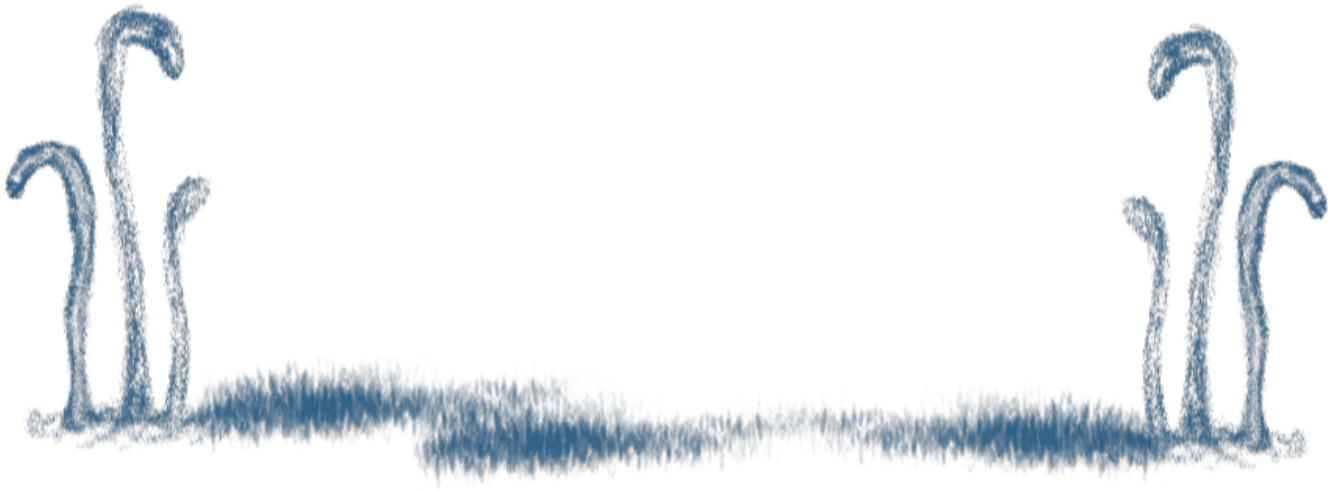
- Defina um bloqueio para imediato que possa ser disparado facilmente
- Tenha uma senha forte
- Criptografe seu telefone
- Criptografe seu cartão SIM

Energia e serviço

E se as pessoas não puderem usar Signal ou outros aplicativos específicos, telefones, Internet, por qualquer motivo - energia, rede ocupada, desligamento etc. Você tem backup ou acesso redundante à Internet - um hotspot de wi-fi portátil, por exemplo (se ele usa dados de celular isso também diminuiria)? Existe um plano offline? Seu hub terá uma estação de carregamento de energia para voluntários?

Recursos adicionais

- Sobre como verificar Números de Segurança e Palavras de Segurança [em inglês] - https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/



Faça Back-up! Bloqueie! Delete! a.k.a. Alguém pegou meu celular: Roubo, encarceramento, acidente, cruzar fronteiras. [atividade práticas]



Nesta atividade, nos planejamos e preparamos para situações em que participantes e seus telefones celulares podem correr risco fisicamente. Possíveis cenários:

- Cuidados ao participar de protestos
- Cuidados ao cruzar fronteiras
- Cuidados quando existe ameaça de encarceramento e risco de acidente
- Cuidados quando existe o risco de roubo e perseguição

Esta atividade é dividida em 4 estágios, com a opção de atividades mão-na-massa de instalação e preparação dos dispositivos. Os estágios são:

- Práticas cotidianas para cuidarmos de nós mesmas
- Planejamento e preparação dos nossos dispositivos
- Interações/Colheita de impressões – opcional

Opcionalmente, encaminhe esta atividade junto com exercícios mão-na-massa para praticar as estratégias e táticas.

Objetivos de aprendizagem aos quais esta atividade responde

- entender sobre cuidados em relação aos telefones celulares desde uma perspectiva de que são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;
- entender dos conceitos básicos de como as comunicações via telefonia celular funcionam para que seus riscos possam ser melhor compreendidos;
- trocar e praticar estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, nossas colegas e nossos movimentos;

Para quem é esta atividade?

Esta atividade é para participantes com variados níveis de experiência em usar telefones celulares para a prática de táticas de segurança com um foco em cuidados e telefones celulares.

Tempo estimado

Esta atividade requer cerca de **80 minutos.**

Recursos necessários para esta atividade

- Papel *flip chart* + canetas marcadoras para documentar a discussão em grupo

Dinâmica

O design deste exercício visa dar suporte para ativistas que estão planejando se engajar em situações que podem ser arriscadas, carregando consigo seus telefones celulares. No final haverá um mapa com ferramentas e táticas que podem ser usadas.

Práticas cotidianas para cuidarmos de nós mesmas – 20 minutos

> ***Nota de cuidados**: Esta atividade é uma atividade tática para planejar e se preparar para o uso de telefones celulares em situações em que as pessoas e seus dispositivos estão em risco. Comece reconhecendo que, para nos prepararmos para uma situação de risco, precisamos primeiro considerar como cuidamos de nós mesmos antes, durante e depois.*

Comece aterrando e discutindo sobre como as pessoas cuidam de si mesmas em situações de alto risco.
Peça a cada pessoa que comece trabalhando por conta própria. Distribua papel e peça-lhes que considerem estas questões e escrevam as suas respostas:

- Em que situações você se envolve em que precisará levar em consideração a sua segurança física e a de seu telefone celular?
- O que você já está fazendo para cuidar de si mesma - antes, durante e depois dessas experiências?

Peça às participantes para dividirem o papel delas em 3 seções: antes, durante e depois.

Desta forma:

Exemplo do papel da participante

ANTES	DURANTE	DEPOIS

Quando no grupo completo, convide as participantes para compartilharem suas práticas. Escreva em um quadro branco ou folha de papel flip chart visível para todo o grupo. Deixe isso em um lugar que seja visível. Peça às pessoas que compartilhem as práticas que fazem individualmente e também com outras pessoas.
As participantes continuarão a usar este mesmo método simples para organizar práticas na próxima parte da oficina.

Planejamento e preparação dos nossos dispositivos – 45 minutos

Se você estiver trabalhando com as participantes se preparando para um evento específico, é melhor já trabalhar com este evento real. Caso contrário, a seguir estão alguns cenários que você pode usar caso as participantes da oficina não estejam se preparando para um evento específico ou caso seu grupo precise de mais base. Estes são alguns exemplos que compartilhamos, sintam-se livres para usá-los sempre que quiserem.

Cenário 1: Cuidados ao participar de protestos

Você está prestes a participar de um protesto em massa. Você precisa ser capaz de manter seus dados do telefone celular seguros e evitar ser rastreada no protesto, mas também precisa ser capaz de usar seu telefone para entrar em contato com aliadas para fins de emergência. Você também está pensando em usar seu telefone para documentar o protesto e quaisquer possíveis violações dos direitos humanos que acontecerão lá.

Cenário 2: Cuidados ao cruzar fronteiras (inseguras)

Você está em trânsito e prestes a cruzar a fronteira para um local inseguro. Você deseja poder usar seu telefone para manter contato com suas aliadas, mas não como um dispositivo de rastreamento pessoal. Pergunte às pessoas quais são suas estratégias quando sabem que outra pessoa pode ter acesso a seus telefones. Exemplos de situações podem incluir passagens de fronteira, embarque em voos, ir a um protesto/manifestação de rua.

Cenário 3: Cuidados quando existe ameaça de encarceramento e risco de acidente

Você ouviu de um contato confiável que está sendo alvo do governo para prisão e apreensão de dispositivos por causa de seu ativismo.

Cenário 4: Cuidados quando existe o risco de roubo e perseguição

Você está preocupada com a possibilidade de alguém roubar seu telefone e usar o conteúdo para assediá-la ou persegui-la.

Peça às participantes para dividirem o papel delas em 3 seções: antes, durante e depois. Desta forma:

Exemplo do papel da participante		
ANTES	**DURANTE**	**DEPOIS**

Em pequenos grupos, ajude as participantes a trabalharem as seguintes conjuntos de perguntas.

Como as pessoas são afetadas: Neste cenário/evento ou experiência para a qual você está se preparando, quais são os riscos? Quem é impactado por isso? Considere você mesmo, as pessoas que estão conectadas ao seu telefone de alguma forma, sua organização/o problema em que está trabalhando (se aplicável).
Você pode usar as perguntas a seguir como perguntas de orientação para que os grupos considerem, de uma forma tática, como reduzir os impactos nas pessoas.

Antes: Pense no que você fará para preparar seu celular para este possível cenário.

- Quais arquivos você excluirá do telefone? Por quê?
- Quais aplicativos você instalará? Por quê?
- Quem você informará sobre seus planos? Quer configurar um sistema de check-in para antes e depois da experiência, é possível?
- Que tipo de comunicação segura você terá com outras pessoas?
- Que outras estratégias você e suas aliadas terão para se manter seguras durante esta experiência?
- Serviços de localização: é mais seguro para você ativar ou desativar a localização e o rastreamento? Você deseja que outras pessoas confiáveis possam seguir sua localização?
- Limpeza remota: deseja ativar a exclusão remota no caso de perder o acesso ao seu dispositivo?

Durante: Pense em como você usará seu telefone durante os acontecimento do possível cenário.

- Energia: a energia é uma preocupação? Como você vai garantir que os telefones celulares das pessoas tenham carga?
- Serviço: o serviço é uma preocupação? O que você fará se as pessoas não puderem usar seu serviço móvel, aplicativos ou dados? Existe um plano *offline*?
- Com quem você deseja se comunicar durante este cenário? Como você se comunicará com elas?

- Você está documentando o protesto? Se sim, você está usando algum aplicativo especial para isso?
- Quem poderá entrar em contato com você pelo seu celular?
- Com quem você entrará em contato pelo seu telefone celular?
- Se precisar usar um cartão SIM diferente do cartão SIM normal, como você escolherá sua operadora? Existe alguma que seja mais segura para sua comunicação? Quem poderá entrar em contato com você? Quem você vai contatar?

Depois: Pense no que você fará após o possível cenário.

- Mídia: se aplicável, o que você fará com as filmagens, imagens, áudio e outras mídias que reuniu?
- Metadados e registros que seu celular faz: quais considerações você precisa fazer sobre os dados que seu telefone está criando durante este cenário? Considere metadados, registros de comunicação, localização de seu dispositivo.
- Em caso de apreensão: como você saberá se seu telefone não foi infectado com *spyware*?
- Em caso de roubo ou apreensão: o que você fará para recuperar a integridade e segurança do seu celular?

Dê aos grupos um mínimo de 30 minutos até um máximo de 45 minutos para que elaborem planos, estratégias e táticas.

No final da discussão em grupo, peça aos grupos para falarem sobre seus planos, estratégias e táticas.

Use os resultados do relatório para planejar sua prática mão-na-massa para segurança dos telefones celulares.

Interações/colheita de impressões (opcional) – 15 minutos

> **Notas de facilitação:** Dependendo do seu estilo e das participantes, você pode querer aprofundar e adicionar contribuições como devolutivas em grupo ou planejar uma seção de contribuições. A seguir estão as notas que acreditamos podem ser úteis para o seu

planejamento.

Antes

- Avise às pessoas que você estará em uma situação em que está preocupada com você mesma e seus pertences pessoais. Faça planos de verificar com uma colega de confiança quando você for entrar e sair dessa situação. Escolha uma frequência destes *check-ins* de verificação que se ajuste aos riscos que você está enfrentando.
- Para uma situação de risco muito alto: Recomendamos que planeje entrar em contato com uma frequência de 10 minutos. Por exemplo, se você estiver indo para um protesto de alto risco ou atravessando uma fronteira particularmente difícil. Planeje dar sinais a cada 10 minutos, ao chegar, enquanto espera (se possível) e ao cruzar a fronteira.
- Para situações de menor risco: Por exemplo, você está em uma cidade trabalhando com um grupo de profissionais do sexo. Você viaja para atender reuniões durante o dia. Faça um plano de verificar com sua amiga de confiança quando você estiver no caminho e quando chegar a cada reunião. Dê notícias também quando você estiver indo dormir, um simples "indo para a cama" e quando você acorda "começando o dia".
- Limpeza de dados: o que há em seu dispositivo que você deseja manter privado?
- Deslogar: saia de todos os serviços nos quais você não precisa estar logada. Não fique conectada a serviços nos quais você não precisa estar conectada. Se alguém pegar seu telefone, essa pessoa poderá acessar suas contas, ver sua atividade e agir como você no serviço se você estiver conectada.
- Bloquear e criptografar: você pode criptografar seu telefone, cartão SD e cartão SIM. Bloquear cada um com um PIN diferente significa que, se alguém tiver acesso ao seu dispositivo, não será capaz de acessar as informações nele ou usá-lo na rede sem o seu PIN. Se você estiver em uma situação em que está sendo ameaçada a dar suas informações de acesso, talvez não consiga manter os PINs e as senhas em sigilo. Discuta com outras pessoas e considere isso ao fazer seus planos de segurança.
- Cópia de dispositivos: muitos órgãos governamentais podem copiar os dados de equipamentos se tiverem acesso a eles, incluindo telefones celulares, laptops, discos rígidos. Se o seu telefone foi copiado mas estiver criptografado, a pessoa que o copiou precisará da sua senha para removê-la. Se o seu telefone não estiver criptografado, a pessoa que o copiou pode acessar todo o conteúdo por meio desta cópia, mesmo que seu telefone retorne a você.

- Fique quieto: desligue sons e gráficos de notificação, mantenha o telefone no mudo.
- Limpeza remota: Você pode ou não querer ativar a limpeza remota. Em algumas situações, você pode querer se preparar para a limpeza remota e garantir que você e uma colega de confiança tenham a capacidade de excluir remotamente o conteúdo do seu telefone se ele for roubado ou perdido.
- Dispositivos e cartões SIM: nossos telefones celulares são dispositivos que criam e transmitem muitas informações, desde mensagens e chamadas que fazemos e enviamos, até dados enviados para aplicativos, e *pins* de localização e hora comunicados com frequência com operadoras de telefonia móvel. Avalie se você deseja transportar seu dispositivo pessoal para uma situação de risco. Se você fizer isso, estas informações de seu dispositivo podem ser conectadas a você e assim você será monitorada continuamente. Em vez disso, você pode escolher deixar seu dispositivo em casa ou usar um dispositivo “descartável”, que não seja vinculado a seu dispositivo usual. Observação: você precisará ter um telefone e um cartão SIM para que isso funcione. Tanto o seu telefone quanto o SIM possuem um ID. Se você usar seu telefone normal e um chip SIM “descartável” e logo substituir o SIM normal após a ação, você ainda será conhecida pelo ID do seu telefone. Esta é uma opção cara, e impedir que um telefone e chip SIM sejam rastreados até você exigirá muito planejamento e a capacidade de parar de usar um dispositivo e destruí-lo. Se você não puder descartar o dispositivo, talvez ainda pense em carregar um telefone alternativo para situações de risco, mas quanto mais você o usar, mais facilmente ele será vinculado a você.
- Removendo cartões SIM: se você estiver entrando em uma situação de risco sem ter um planejamento, você pode querer remover partes sensíveis do seu telefone, como o chip SIM e o cartão de memória (se possível). Nota: em algumas situações, isso pode ser usado como uma desculpa pelos agressores para aumentar o dano.

Durante

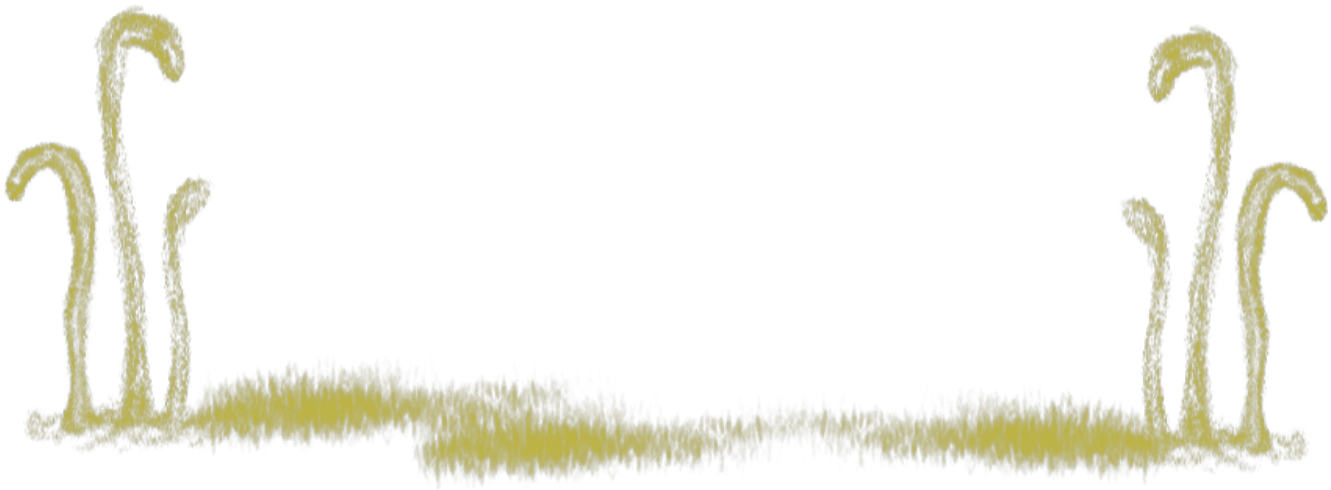
- Limpeza remota
- PixelKnot para mensagens criptografadas
- Briar para protestos e desligamentos de rede

Depois que seu telefone estiver ficado fora de seu controle

- Limpe-o ou compre um novo dispositivo: se você puder pagar, substitua o dispositivo; compre um novo e mande o antigo para alguém que possa analisá-lo. Caso contrário, nossa melhor recomendação é formatá-lo para as configurações de fábrica.
- Seus serviços: redefina as senhas de todos os seus serviços.
- Informe as pessoas: se o seu telefone estiver fora de seu controle, informe seus contatos e pessoas com quem você se comunicou ativamente e quais podem ser as implicações para elas.

Recursos adicionais

- EFF Defesa Pessoal contra Vigilância | EFF Surveillance Self Defense [em inglês]:
- Encripte seu iPhone https://ssd.eff.org/en/module/how-encrypt-your-iphone
- Usando Signal no iPhone - https://ssd.eff.org/en/module/how-use-signal-ios
- Usando Signal no Android - https://ssd.eff.org/en/module/how-use-signal-android
- Usando Whatsapp no iPhone - https://ssd.eff.org/en/module/how-use-whatsapp-ios
- Using Whatsapp no Android - https://ssd.eff.org/module/how-use-whatsapp-android



Discussão, interações + mão-na-massa: Escolhendo aplicativos móveis [atividade práticas]



Esta é uma atividade de discussão e interação que tem como foco permitir que as participantes escolham os aplicativos móveis por elas mesmas, especialmente depois da oficina.

Esta atividade tem 3 estágios:

- Discussão: O que você está usando e por quê?
- Interações/colheita de ideias e impressões: Boas práticas ao escolher aplicativos
- Atividade mão-na-massa: Avaliação de aplicativos de mensagens **OU** Atividade mão-na-massa: Avaliação de aplicativos populares

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento sobre cuidados em relação aos telefones celulares desde uma perspectiva de que eles são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;
- realizar trocas e praticar estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, colegas e nossos movimentos.

Para quem é esta atividade?

Esta sessão se aplica a qualquer pessoa que já usou um telefone celular e quer manejar melhor como fazer as escolhas de aplicativos.

> **Marcadores de diferença:** esta atividade é desenhada como uma prática para avaliar a segurança de aplicativos móveis, especificamente aplicativos de mensagens instantâneas. Outros tipos de aplicativos que podem ser também relevantes para as participantes são:

- aplicativos de menstruação/fertilidade e os dados que eles coletam e as soluções de controle de natalidade que oferecem
- aplicativos de namoro/paquera
- aplicativos de mensagens/chamadas de emergência e aplicativos de apagamento remoto/restauração imediata de dispositivos, ex.: funções de buscar telefone para Android e iPhone
- aplicativos de segurança voltados para vigilância (ex.: acesso remoto, babá eletrônica, software "espião")
- jogos ou outros aplicativos com componente interativo
- aplicativos performativos como o TikTok

Tempo estimado

Esta atividade requer cerca de **60 minutos.**

Recursos necessários para esta atividade

- Papel para grupos pequenos escreverem anotações
- Quadro branco ou papel grande para anotar anotações partilhadas
- Alguns telefones celulares com pacote de dados e loja de aplicativos (ex.: Play Store)

Dinâmica

Discussão: O que você está usando e por quê? - 10 minutos

Em plenária, pergunte: Quais são os 5 aplicativos que você mais usa? Para que você os usa? Faça com que todas contribuam para a discussão.

- Liste os aplicativos na medida em que as participantes os mencionam, pergunte quem mais os usa e marque o número de usuárias de cada aplicativo que estão na sala
- Liste as razões pelas quais elas os utilizam

Então pergunte: Como vocês escolheram estes aplicativos?

- Escreva as respostas sobre como elas escolhem os aplicativos que usam e

Para sintetizar, sumarize as razões e some-as às sugestões colhidas com o grupo.

Interações/colheita de ideias e impressões: Melhores práticas para escolher aplicativos – 5 minutos

- Pesquisa! Saiba mais sobre as opções, saiba qual aplicativo é confiável. Peça às participantes que compartilhem seus métodos de pesquisa – ex.: você pode ler sobre isso em algum lugar *online/offline*, pergunte a uma amiga que você conhece que gosta de pesquisar. Leia comentários positivos e negativos no centro de download.

- Como você começa a ter certeza de que é um aplicativo seguro? Quem o desenvolve? Qual é a política de privacidade deles? É código aberto? Houve incidentes com o aplicativo sendo usado para obter acesso aos sistemas?
- Compreender as permissões que os aplicativos exigem. Por exemplo, por que um aplicativo de jogo precisa acessar sua câmera ou contatos?
- O que faz você se sentir mais segura/confiante ao usar o aplicativo - você pode controlar as permissões? Você sabe onde ele armazena informações sobre você ou que você gera com o aplicativo? / Você sabe para onde as coisas vão?
- Se este for um aplicativo social, como você deseja interagir com as pessoas neste aplicativo? O que você pode escolher sobre para quem você é visível, o que é visível para as pessoas, como as pessoas podem interagir com você e como você pode interagir com elas? Quais são as configurações padrão, o que elas revelam sobre você, com quem elas conectam você? Você conhece algum problema de segurança nesta ferramenta? Existem mecanismos de reclamações/sugestões que você pode usar? Isso poderia ser usado contra você?

Atividade mão-na-massa: Avaliação de aplicativos populares – 15 minutos

Vá até a loja de aplicativos e tente encontrar um aplicativo de uso corriqueiro. Em um ambiente urbano, talvez um aplicativo de chamada de táxi, mapa do sistema de metrô etc.

Como você escolhe? Verifique (1) quais permissões ele pede (2) quem está distribuindo o aplicativo e quem gerencia e é proprietário do serviço. Existem muitos aplicativos por aí que são cópias de aplicativos populares, feitos para se parecer com algo que você deseja, como um jogo ou um mapa do metrô, e eles são projetados para fazer outras coisas, como enviar sua localização para outra pessoa. O desenvolvedor ou empresa que está distribuindo o aplicativo será nomeado na loja de aplicativos. Compartilhe o que você sabe sobre quem é o proprietário/administra o serviço e pesquise as maneiras pelas quais os valores embutidos no aplicativo são semelhantes e/ou diferentes dos seus e como isso pode afetar sua privacidade e segurança ao usar o aplicativo. Se você estiver escolhendo entre vários aplicativos que parecem iguais, procure em outro lugar online para obter mais informações sobre o aplicativo e quem é o desenvolvedor ou empresa que o distribui e verifique se você está baixando o correto.

Atividade: Avaliação de aplicativos de mensagens – 30 minutos

Divida as pessoas em grupos menores. Nos pequenos grupos:

- identifique 2 ou 3 aplicativos de mensagens instantâneas que estão sendo mais utilizados nesse pequeno grupo
- responda as questões guias/sugeridas

Em plenária: Faça a devolutiva, cada grupo compartilha um aplicativo até que todos os aplicativos citados sejam vistos coletivamente.

Questões guias/sugeridas:

- Quem, entre as participantes, usa este aplicativo? É fácil de usar?
- Quem é dono do aplicativo? Quem gerencia o serviço?
- Onde suas mensagens são armazenadas?
- Está criptografado? Que outras configurações de proteção e segurança ele possui? De que outras maneiras você mantém sua comunicação segura ao usar este aplicativo?
- Quando é bom usar?
- Quando é melhor não usar?

Lista de aplicativos de mensagens instantâneas e considerações

SMS

- Todas usam SMS
- Empresa de telefonia móvel. Particularmente arriscado se houver histórico de conluio entre telco e governo, ou se for uma telco de propriedade do governo ou se a empresa for corrupta.
- Armazenado pela operadora de serviço móvel – existem diferentes políticas de armazenamento de mensagens. Mensagens transmitidas através de torres entre você e a pessoa por meio da qual você está enviando as mensagens.
- Sem criptografia.

- Bom para comunicação de assuntos que não são arriscados/confidenciais.
- Frequentemente existe um custo por mensagem.

Ligações

- Todas fazem
- Operadoras de serviços móveis têm controle sobre elas.
- Armazenadas pelas operadoras de serviços móveis – com certeza pelo menos os metadados.
- Exemplo de insegurança: Apenas nos últimos 5 anos, diversos casos de interceptação telefônica ultrapassaram o limiar das investigações e se tornaram exemplos de ferramenta de manipulação política, incluindo o fatídico "Tchau, querida" entre Lula e Dilma.
- Bom para comunicação de assuntos que não são arriscados/confidenciais.
- Frequentemente existe um custo por mensagem.

Facebook Messenger

- Qualquer pessoa com uma conta FB pode usá-lo.
- Vem com seu próprio aplicativo
- Criptografia prometida, mas não verificada
- O Facebook é o dono
- Em vez de usar o aplicativo FB, use o Chat Secure. Você pode usar suas credenciais do FB para bater papo com outros usuários do FB. Mas para que a criptografia funcione, as pessoas com quem você está conversando também precisam usar o Chat Secure e se comunicar com você pelo Chat Secure.
- Frequentemente gratuito, entretanto, requer uma conexão de internet ou pacote de dados.

Google Talk

- Qualquer pessoa com uma conta do Google
- Vem com seu próprio aplicativo
- Criptografia prometida, não verificada
- O Google é o dono
- Você também pode usar o Chat Secure para acessá-lo.

Signal (aplicativo recomendado)

- Administrado por ativistas de tecnologia
- Criptografia ponta a ponta
- Sem armazenamento em nuvem. Você armazena mensagens em seu telefone ou computador, o Signal não armazena mensagens depois que foram entregues.
- Também possui ligações criptografadas
- Usado para comunicações sensíveis

Telegram

- Aplicativo de mensagens instantâneas popular
- Criptografia ponta a ponta somente nos chats secretos

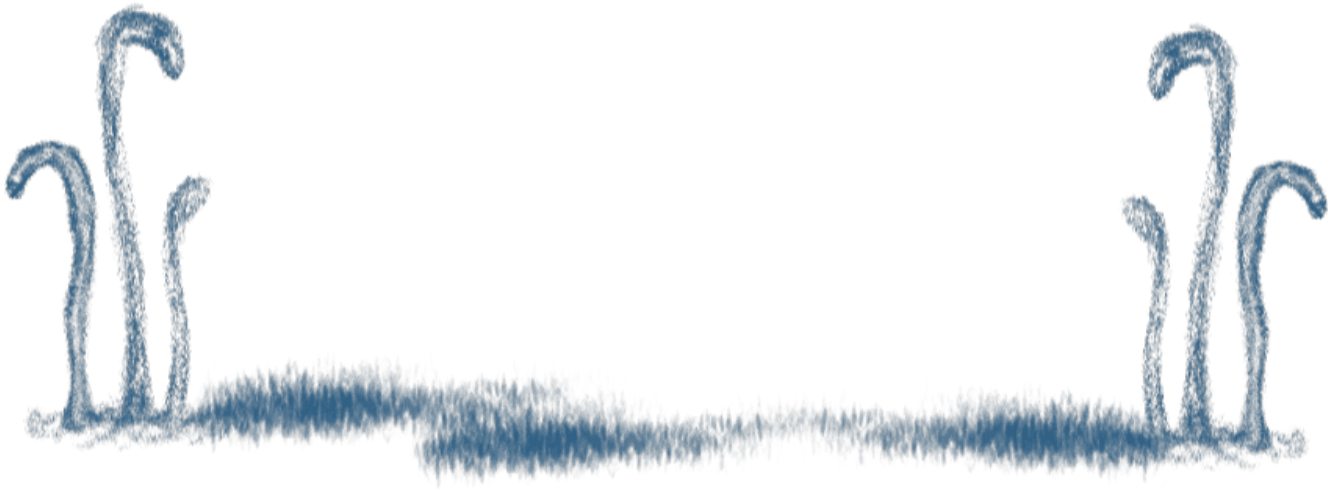
WhatsApp

- Muito utilizado
- O Facebook é dono do WhatsApp, embora os desenvolvedores do WhatsApp prometam salvaguardar a privacidade dos usuários em sua Política de Privacidade
- Armazena apenas mensagens ainda não entregues.
- Criptografia ponta a ponta, mas se o backup das mensagens for feito no e-mail associado, elas serão armazenadas sem criptografia.
- Bom para se comunicar com muitas pessoas
- Existem preocupações pelo fato de ser propriedade do FB

Recursos adicionais

- O que é criptografia - https://myshadow.org/alternative-chat-apps#end-to-end-encryption-amp-perfect-forward-secrecy [em inglês]
- Aplicativos de Chat Alternativos: https://myshadow.org/alternative-chat-apps [em inglês]
- Por que Signal e não Whatsapp?
- Dicas da EFF, Ferramentas e Como fazer para ter Comunicações Online mais Seguras - https://ssd.eff.org/pt-br
- Também é uma boa ideia fazer uma pesquisa na web sobre os problemas de segurança mais recentes com os aplicativos nos quais você planeja usar na oficina e sugerir. As

palavras-chave a serem usadas são: nome do aplicativo + análise de segurança + ano ou nome do aplicativo + problemas de segurança conhecidos + ano . Dependendo do que encontrar, você pode querer remover um aplicativo com problemas de segurança conhecidos e não resolvidos da sua lista de aplicativos usada na oficina.



Usando dispositivos móveis para documentar violência: Planejamento e prática [atividade práticas]

Esta é uma atividade tática para ativistas que pretendem usar seus telefones celulares para documentar a violência. As participantes farão práticas de uma avaliação de segurança e um plano de documentação. As participantes colocarão a mão-na-massa com seus telefones celulares para praticar a documentação usando seus aplicativos e ferramentas escolhidas.



Esta é uma **atividade tática** para ativistas que pretendem usar seus telefones celulares para documentar a violência. As participantes farão práticas de uma avaliação de segurança e um plano de documentação. As participantes colocarão a mão-na-massa com seus telefones celulares para praticar a documentação usando seus aplicativos e ferramentas escolhidas.

> ***Nota de cuidados:*** *Facilitadoras, esta é uma atividade longa e pode tomar quase um dia todo. Assegure-se de fazer pausas ao longo do processo. Reconheça que o ato de documentar é estressante e encoraje suas participantes a partilharem exercícios que elas acham que facilitam este processo de documentação, por exemplo, exercícios motores e de*

> *respiração.*

Esta atividade tem 2 partes:

Parte 1: Avaliação e Planejamento
Primeiro as participantes irão planejar o trabalho, avaliando questões de segurança e o bem-estar das envolvidas. Com base nessa avaliação, farão planos de segurança e tomarão decisões sobre o gerenciamento de telefones celulares e mídia.

Parte 2: Configurações e Práticas
Em seguida, as participantes irão praticar táticas para documentar a violência usando telefones celulares.
Recomendamos também usar a atividade de aprofundamento Debate: Documentação de violência

Objetivos de aprendizagem aos quais esta atividade responde

- realizar trocas e praticar estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, colegas e nossos movimentos.

Para quem é esta atividade?

Grupos que já usem ou estejam considerando usar telefones celulares para documentar violência.

Tempo estimado

Esta atividade requer cerca de **1 hora e 45 minutos.**

Recursos necessários para esta atividade

- Estudos de caso impressos ou links

Dinâmica

Introdução – 5 minutos

Compartilhe alguns exemplos recentes de movimentos que usam celulares para documentar violência e peça às participantes que compartilhem exemplos de como elas estão usando celulares para documentar violência ou para compartilhar a documentação. Os exemplos podem incluir: documentar violência do Estado, encaminhar vídeos de atos violentos, as possíveis implicações de ter a posse desse tipo de mídia.

Parte 1: Avaliação e planejamento – 30 minutos

Facilite que as participantes se dividam em pequenos grupos baseadas em situações similares que elas estejam vivenciando quando documentam violências.

> ***Nota de cuidados:*** *Facilitadoras, encorajem as participantes a avaliar e planejar suas próprias necessidades de cuidados. Documentar atos de violência pode ser estimulante e estressante para quem documenta. Incentive as participantes a compartilharem como elas obtêm recursos próprios, como estão trabalhando com outras ativistas para lidar com os impactos da documentação.*

> ***Veja também a Atividade Tática*** Faça Back-up! Bloqueie! Delete! a.k.a. Alguém pegou meu celular: Roubo, encarceramento, acidente, cruzar fronteiras***.***

Objetivo e planejamento: Discuta o objetivo da documentação

• O que você está documentando e por quê?
• Qual é a situação?

• Qual é o propósito da sua documentação? Se for para ser usado como evidência, planeje-a de acordo com os requisitos para que ela possa ser aceita como evidência. Para obter mais informações, consulte Recursos de vídeo como evidência da WITNESS: https://portugues.witness.org/tutoriais/video-como-evidencia/

Avaliação de riscos e cuidados: Discuta problemas de segurança já conhecidos e prováveis que aconteçam para as pessoas que estão documentando e sendo documentadas

- Quais são os prováveis problemas de segurança que você enfrentará durante este trabalho? É provável que você encontre policiais ou antagonistas/oponentes?
- O que pode ser mudado em relação ao seu contexto, o que afetará sua segurança e como você planejará isso? Discuta alguns cenários prováveis. Os exemplos podem incluir polícia e outros antagonistas/oponentes se tornando mais agressivos ou violentos. As respostas podem incluir continuar a documentar, aumentar a frequência de verificações de segurança entre sua equipe, interromper o processo de documentação.
- Quem participará da documentação (filmagem, suporte, comunicações etc.) e que suporte essas pessoas têm e de que qual precisam?
- O que você sabe sobre questões de segurança - alguém em nossa grupo se sente mais ou menos segura em participar com base no conteúdo ou contexto desta documentação? Quais funções elas se sentem confortáveis em assumir?
- Que estratégias você e suas aliadas adotarão para se manterem seguras durante a documentação?
- Qual é o papel do consentimento nesta documentação? Você buscará o consentimento das pessoas que documentar e como elas consentirão em serem filmadas ou documentadas? Você buscará o consentimento daquelas que você documenta em relação ao compartilhamento dessa filmagem e documentação mais tarde?
- Quais são os problemas de segurança relacionados ao fato de você possuir esta filmagem? Quais são os problemas de segurança para as pessoas que aparecem na filmagem? Como você cuidará da filmagem depois que ela for filmada e armazenada em seu dispositivo, no armazenamento secundário? Considere onde você irá armazená-lo, quem tem acesso, se o armazenamento está criptografado, quando você irá excluí-lo.

- Como você pode ser impactada por documentar a violência? De quais recursos você precisa para estar bem e ter os pés no chão ao fazer este trabalho? Que recursos os outros poderiam fornecer? Como você e sua equipe apoiarão umas às outras em suas necessidades individuais de recursos e o que podem fazer juntos para apoiar umas às outras?

Conheça seus direitos

- Baseada na legislação de onde você se encontra, quais são seus direitos em relação à documentação?
- Como isso se relaciona com o contexto de sua documentação? Exemplos de perguntas que você pode fazer: é legal filmar policiais, assembleia pública é legal?
- A polícia tem permissão para revistar seus dispositivos?
- A polícia vasculha dispositivos ou força as pessoas a deletarem mídia?

Preparando seu dispositivo

- Você está usando seu celular pessoal?
- Quais arquivos você deve excluir do telefone? Por quê?
- Quais aplicativos você deve instalar ou desinstalar? Por quê?
- Serviços de localização: é mais seguro para você ativar ou desativar a localização e o rastreamento? É vantajoso que você tenha colegas que possam ser capazes de seguir sua localização?
- Você deseja ativar a limpeza/exclusão remota no caso de perder o acesso ao seu dispositivo?

Discussão: Por que ou por que não você usa seu celular pessoal para documentar violência?

Interações

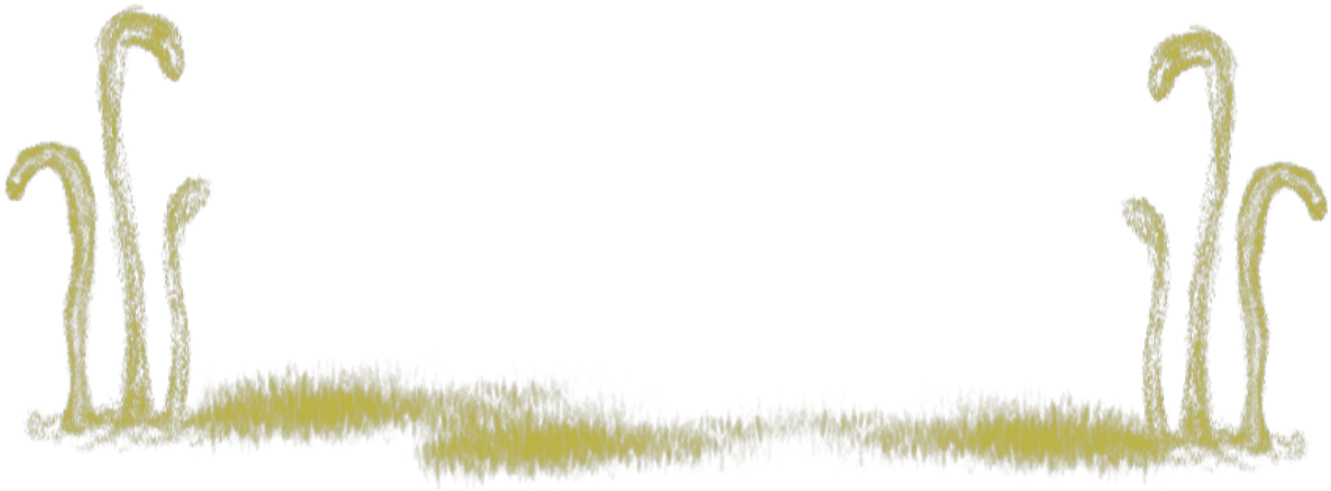
Use informações da **Atividade de Planejamento:** **O que é um telefone? Como as comunicações móveis funcionam?** para explicar como os telefones celulares estão ligados às pessoas que os usam, como a identificação funciona com vigilância em tempo real, como os metadados sobre o uso do telefone e os dados EXIF de mídia podem ser usados para te identificar.

Depois

- Faça um plano de reunir as participantes para uma devolutiva. Como foram as coisas? Que coisas inesperadas aconteceram e como a sua grupa respondeu? O que ainda precisa de resposta? Como estão as pessoas e quem participará das próximas etapas?
- Compartilhamento - analise seus acordos sobre consentimento e compartilhamento. Certifique-se de compartilhar esses acordos com qualquer outra pessoa com quem trabalhará para compartilhar a filmagem.

Discussão

O que mais você deseja fazer após a documentação?



Parte 2: Configurações e práticas - 60 minutes

Dependendo da disponibilidade de tempo que tiver, você pode fazer todas estas atividades ou separá-las em pequenos grupos de forma que as pessoas se juntem e façam as atividades de acordo com suas próprias necessidades.

Dicas e truques de gravação

Como usar foto, vídeo e / ou gravação de áudio para documentar a violência:

- Encontre as ferramentas integradas em seu telefone para gravação: fotos, vídeo, áudio
- Pratique o uso dessas ferramentas, considere as dicas da WITNESS sobre as filmagens em equipe e usando o celular (link nos recursos abaixo)
- Planeje suas filmagens, seja seletivo
  - Captura de detalhes e perspectiva: aproxime-se fisicamente para registrar mais detalhes e volte para mostrar uma perspectiva mais ampla dos eventos
  - Mantenha suas fotos estáveis: escolha sua foto e segure firme por pelo menos 10 segundos, evite o zoom, use as duas mãos e mantenha os cotovelos contra o corpo para estabilidade extra
  - Segure seu telefone horizontalmente para capturar um ângulo mais amplo
  - Aproxime-se para um bom som: esteja ciente de ruídos altos que podem abafar as entrevistas
  - Esteja atento à iluminação: grave em um local bem iluminado e mantenha o sol e as luzes fortes às suas costas

- Se você tiver tempo, trabalhe em equipes para planejar a documentação já usando essas ferramentas. Pratique criando uma mídia.
- Se você for compartilhar no YouTube, considere usar o recurso de legenda: https://support.google.com/youtube/answer/2734796?hl=pt-BR
- Contexto e mensagens. Planeje sua mensagem. Onde você postará isso e que texto postará para acompanhá-la? Como você vinculará isso aos seus objetivos maiores?

Gravando chamadas telefônicas

Entrada

Isso provou ser útil para profissionais do sexo que estavam sendo ameaçadas por autoridades.

Usando um aplicativo

Você pode instalar e usar um aplicativo que te permite gravar. Isso exigirá dados para download e dados para realização da chamada, pois o aplicativo usará dados e não a linha telefônica e levará algum planejamento prévio.

- Avalie qual aplicativo você gostaria de usar e instale-o

    - O Google Voice permite que você grave chamadas recebidas, não chamadas efetuadas
    - Seu celular pode ter um aplicativo de gravação integrado
- Teste com uma parceira
- Pratique como localizar a mídia e salvá-la de seu telefone em um local seguro onde você possa acessá-la quando precisar.

Usando um gravador

Se por algum motivo você não puder ou decidir por não usar um aplicativo, você tem opções de gravar usando um gravador ou pedir ajuda para gravar com o celular de outra pessoa. Você pode usar seu telefone no viva-voz e gravar usando um dispositivo de gravação de outra pessoa, ou usar o telefone dela como gravador de voz para gravar a chamada. Alguns telefones possuem um recurso de gravação de voz integrado.

- Avalie qual ferramenta ou aplicativo você gostaria de usar e instale-o
- Teste com uma parceira. Para obter o melhor som, aproxime-se e grave em um local longe de outros sons altos.
- Pratique como localizar a mídia e salvá-la de seu telefone em um local seguro onde você possa acessá-la quando precisar.

Capturas de tela

Você pode fazer capturas de tela do seu telefone para documentar quando o assédio e a violência acontecem via mensagens de texto.

- Escolha um aplicativo para capturar imagens e praticar:
    - No Android: um telefone que usa a versão Android Ice Cream Sandwich, você pode pressionar o botão de diminuir volume e liga/desliga ao mesmo tempo, segure por um segundo e seu telefone fará uma captura de tela que é salva na sua galeria.
    - iPhone X, XS, XR: Pressione e segure o botão lateral à direita e clique no botão Aumentar volume ao mesmo tempo e seu telefone fará uma captura de tela que é salva em seus álbuns em um álbum chamado Screenshots.
    - iPhone 8 e anterior: Pressione e segure o botão liga/desliga no lado direito e clique no botão inicial ao mesmo tempo. A captura de tela será salva em um álbum chamado Screenshots.

- Pratique como localizar a mídia e salvá-la de seu telefone em um local seguro onde você possa acessá-la quando precisar.

Tenha em mente que você não poderá capturar a tela de todos os aplicativos. Alguns aplicativos, como o Signal, têm uma configuração de segurança que permite ao usuário impedir que outros capturem a tela de conversas específicas.

Documentar os eventos para registros internos

Conforme um incidente está ocorrendo, seja ele breve, longo, acontecendo pela primeira vez ou reincidente, é importante documentar as informações sobre o evento. Considerando que muitas das outras táticas giram em torno da documentação para compartilhamento público e social, isso pode ser útil principalmente como uma prática interna. Onde o evento está ocorrendo, quando, quem está envolvido, o que está acontecendo. Manter o controle dessas informações pode ser útil na reconstrução de eventos, avaliação e planejamento de respostas.

Transmissão AO VIVO

Adaptado do material da WITNESS: Como fazer transmissão ao vivo em protestos (EUA) – How to Livestream Protests (US) https://library.witness.org/product/livestreaming-protests-usa/ [em inglês].

Você está transmitindo ao vivo em um evento como um protesto, manifestação, etc. Esteja certa de usar as atividades de Avaliação e Planejamento. Transmissão Ao Vivo pode ser uma ótima maneira de mostrar os eventos que estão ocorrendo e de envolver as pessoas que estão assistindo e apoiando. Também existem alguns riscos elevados, pois pode haver presença da polícia no protesto e ainda pode haver policiais observando ao vivo ou após a gravação, na intenção de identificar e criminalizar as ativistas.

- **Localização:** Documente sua localização intencionalmente. Filme placas de rua, prédios, e pontos de referência para documentar sua localização. Ainda, considere como revelar a sua localização em tempo real compromete sua segurança e a das pessoas que você está filmando.
- **Identificação de participantes:** Você será capaz de obter o consentimento das pessoas que está filmando? Como você quer e precisa proteger as identidades delas? Considere não filmar rostos.

- **Identificação de táticas:** Esta é uma faca de dois gumes. Você pode acabar filmando, sem intenção, as táticas das ativistas de uma maneira que possa impactá-las negativamente. Ao mesmo tempo, você pode documentar táticas da polícia para que possa avaliar melhor suas formações e prováveis ações futuras.
- **Para quem transmitir:** Quais são as suas metas em transmitir ao vivo? Você quer transmitir primeiro para um pequeno grupo de pessoas confiáveis para que elas possam te dar suporte retransmitindo sua mídia?
- **Trabalhe em grupo:** Trabalhe junto com outras que possam te dar suporte através do engajamento de audiência nos comentários e discussões, e que possam repostar a mídia em múltiplos canais.
- **Faça demandas:** Busque o engajamento de sua audiência para ação.
- **Seu dispositivo:** Você quer usar seu dispositivo pessoal? Qualquer dispositivo que usar, encripte-o e proteja-o com uma senha. Não use o desbloqueio por impressão digital.

Devolutiva - 10 minutos

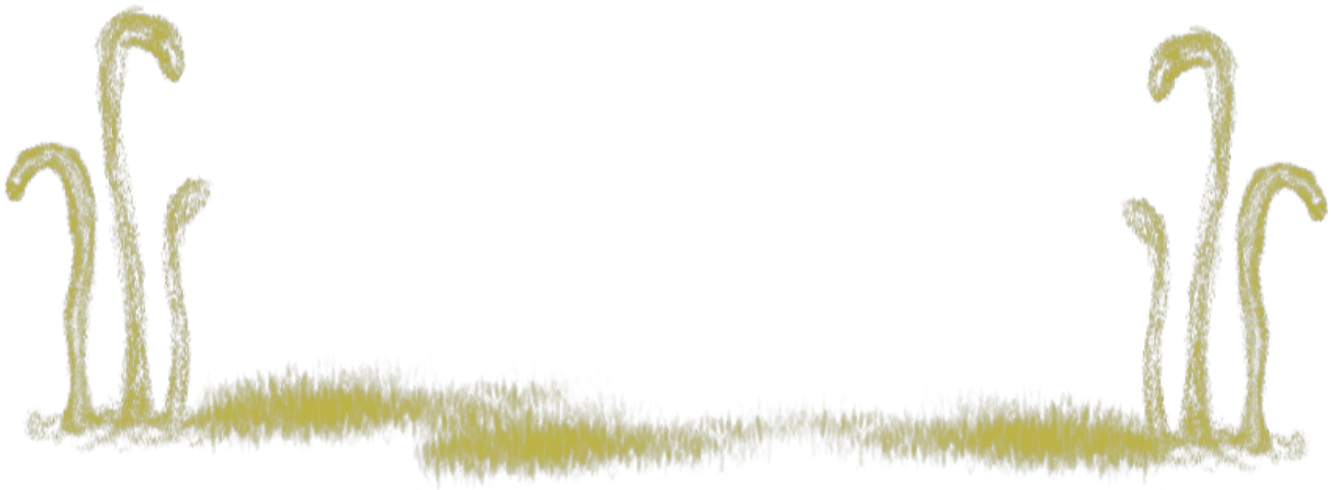
- Ancore a devolutiva numa conversa sobre o porquê documentamos violências. Reconheça que este é um trabalho estressante.
- Compartilhe qualquer mídia que os grupos tenham criado quando estavam separados.
- Compartilhe qualquer aprendizagem, novas ferramentas e dicas que tenham sido colocadas pelas participantes.

Recursos adicionais

- Rede Vídeo para Mudança (Video For Change Network) - https://video4change.org/ [em inglês]
- WITNESS – Filmagem em Equipe: Protestos, Manifestações e Atos - https://portugues.witness.org/portfolio_page/filmagem-em-equipe/
- WITNESS – Filmando com um Celular - https://portugues.witness.org/portfolio_page/filmando-com-um-celular/
- WITNESS - Guia prático para entrevistar sobreviventes de violência sexual e de gênero - https://blog.witness.org/2013/08/new-how-to-guide-for-interviewing-survivors-of-sexual-and-gender-based-violence/ [nota da tradutora: Versão em Português em andamento e

em Espanhol disponível em: https://www.mediafire.com/folder/2h9lnjn685404/Spanish]

- WITNESS – Como fazer transmissão ao vivo em protestos https://portugues.witness.org/tutoriais/video-como-evidencia/
- O que são metadados em vídeo? (What is Video Metadata?) https://library.witness.org/product/video-metadata/ [em inglês]
- UWAZI- https://www.uwazi.io/ [em inglês] - Uwazi é uma solução gratuita e de código aberto para organizar, analisar e publicar seus documentos.



Reinicie sua segurança em aplicativos de paquera online [atividade práticas]



Esta é uma **atividade tática** na qual as participantes compartilham dicas e truques para paquera online.

As participantes trabalharão em pequenos grupos ou em pares para atualizarem seus próprios perfis e práticas em aplicativos de paquera.

As participantes compartilharão suas diferentes necessidades e preferencias em relação aplicativos de encontros/paquera, privacidade e segurança.

As participantes compartilharão e praticarão diferentes táticas a fim de aumentar a privacidade no uso de seus aplicativos de encontros/paquera.

> ***Nota Interseccional:*** *Facilitadoras, abram espaço para as pessoas compartilharem como suas considerações e práticas de paquera online se relacionam com seu gênero e sexualidade. Dentre as participantes, como o gênero e a sexualidade se relacionam com os aplicativos que as pessoas estão usando para paquerar? Como eles se relacionam com as preocupações existentes sobre privacidade e segurança?*

Esta atividade tem 2 partes:

- Compartilhar dicas e truques de paquera online e segurança
- Mãos-na-massa: Reinicie sua segurança em encontros/paquera online

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento de como o acesso a comunicações móveis é diferenciado por gênero e é íntimo;
- um entendimento sobre cuidados em relação aos telefones celulares desde uma perspectiva de que eles são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;
- realizar trocas e praticar estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, colegas e nossos movimentos.

Para quem é esta atividade?

Pessoas que estejam utilizando aplicativos de encontros/paquera e querem usá-los com mais segurança.

Tempo estimado

Esta atividade requer cerca de **2 – 2.5 horas.**

> **Nota para facilitadora:** Este exercício leva cerca de 2,5 horas e nós recomendamos fazer algumas pausas durante o trabalho.

Recursos necessários para esta atividade

- Acesso à Internet

- Telefones celulares para atualizar os perfis dos aplicativos de encontros/paquera online
- Flip chart ou quadro branco

Dinâmica

Compartilhar dicas e truques de paquera online e segurança

Quebra gelo - 5 minutos

- Quem está usando apps de encontros/paquera online, quais? Como você os escolheu e por quê?
- De que formas você já pensa e cuida da sua segurança e privacidade?

Paquera/Encontros mais segura – 30 minutos

Antes de entrar nos aplicativos e atividades mãos-na-massa com os dispositivos, facilite a partilha de dicas no uso de aplicativos de paquera entre as participantes.

Pergunte:

- Como é um comportamento seguro para você quando está usando aplicativos de paquera/encontros online?
- O que você considera para decidir se irá encontrar alguém cara-a-cara?
- Quais são as suas estratégias para saber se é seguro encontrar determinada pessoa?
- Você tem um plano B para quando as coisas dão errado? Tem um tempo de *chek-in* combinado com uma amiga? Ou avisa uma amiga aonde você está indo, com quem irá se encontrar, etc.?

Escreva as respostas num flip chart ou em algum lugar visível para as participantes.

Compartilhe estas dicas de segurança adicionais e peça as participantes para compartilharem e adicione:

Aplicativos de paquera (dicas de segurança)

- Se assegure que sua foto não dará nenhuma informação extra a seu respeito, especialmente relacionada à sua localização, à escola que estuda
- Use um e-mail específico e seguro
- Não use um nome de usuária que seja similar ao de outras contas em redes sociais
- Use uma foto de perfil que seja diferente das usadas em seus perfis de redes sociais
- Não use informações pessoas
- Seja cuidadosa e pense bem sobre quando irá fazer seu perfil nos aplicativos de paquera
- Encontro Offline: encontre a pessoa num local público pela primeira vez. Se possível, informe uma amiga/familiar sobre o local e a hora deste encontro.
- Configure uma senha nos seus aplicativos quando possível
- Encripte e coloque senha de bloqueio de tela no seu dispositivo

Interações: Novos modelos de namoro/paquera

Há alguma caraterística que lhe agrade particularmente nas aplicações de encontros existentes e que possa procurar nas novas aplicações?

Que possibilidades e características oferecem as novas aplicações (por exemplo, sinalizar de alguma forma os utilizadores com má reputação, documentar os burlões, partilhar dicas de encontros)?

Como é que já interage com os seus amigos de confiança e membros da sua comunidade de encontros em linha?

Mãos-na-massa: Reinicie sua segurança em encontros/paquera online - 60-90 minutos

Comece por fazer um leve “*Doxxing*” de você mesma – veja quais informações estão disponíveis sobre seu nome em seus apps de paquera. Usando a informação obtive através do seu perfil no aplicativo, busque a si mesma em outras plataformas. Tente procurar pelo seu nome ou informações que você partilhou no seu perfil. Reflita sobre quais as informações sobre você que estão disponíveis fora dos aplicativos e que você gostaria que as pessoas dos aplicativos não tivessem acesso. Com base nisso, refaça seu perfil.

> **Nota da tradutora:** Doxxing é a prática de coletar informações pessoais de uma pessoa ou mais pessoas e divulgá-las com a intenção de causar mal, gerar ataques virtuais, exposição e gerar prejuízos sociais e financeiros. No contexto utilizado, trata-se de uma leve ironia, sugerindo que você utilize várias práticas geralmente utilizadas pelas pessoas que praticam doxxing em si mesmas e possa assim verificar que tipos de informações podem ser encontradas sobre você nas redes e quais delas podem ser utilizadas para te prejudicar.

Em duplas, siga as dicas de segurança e atualize seu perfil. Compartilhem entre si os perfis e dê suporte à sua parceira apontando se existem informações que a identifiquem ou se elas podem mudar mais elementos para que possam ser menos identificadas, e assim atenderem às próprias metas de segurança.

Renove suas fotos

Reveja e substitua quaisquer imagens, incluindo as do seu perfil e de outras contas, se elas não atenderam as dicas de segurança que você quer seguir. Considere remover metadados que possam te identificar e remover informações reveladoras sobre outras pessoas nas imagens.

Renove seus textos

Reveja e reescreva seu texto se ele estiver revelando mais informações que você gostaria, considerando sua segurança. Faça esta reescrita com uma parceira se quiser!

Configure separadamente um e-mail seguro.

Devolutiva - 10 minutos

Como foi fazer isso? O que foi surpreendente? O que foi fácil? O que foi difícil? Quais serão os próximos passos?

> **Facilitatoras:** As participantes estão interessadas em *sexting*? Veja o módulo de *sexting* mais seguro.

Recursos adicionais

Privacidade e segurança em contextos conservadores: os apps de encontros para mulheres da diversidade sexual (Privacidad y seguridad en contextos conservadores: las apps de citas para mujeres de la diversidad sexual. Steffania Paola): https://www.genderit.org/es/articles/edicion-especial-privacidad-y-seguridad-en-contextos-conservadores-las-apps-de-citas-para [em espanhol]

Self-Doxxing: https://gendersec.tacticaltech.org/wiki/index.php/Step_1#Self-Doxing

Recursos de Segurança nos apps de paquera/pegação [em inglês]

- Grindr - https://help.grindr.com/hc/en-us/articles/217955357-Safety-Tips
- Planet Romeo - https://www.planetromeo.com/en/care/online-dating/
- Tinder - https://www.gotinder.com/safety
- OKCupid - https://www.okcupid.com/legal/safety-tips
- Hornet - https://hornet.com/community/knowledge-base/tips-on-how-to-stay-safe/
- Scruff: http://www.scruff.com/gaytravel/advisories/



Manda nudes, só que mais segura [atividade práticas]



Esta é uma **atividade tática** na qual participantes trocam em si e praticam táticas para praticar todas as formas de *sexting* um pouco mais seguras.

Objetivos de aprendizagem aos quais esta atividade responde

- um entendimento de como o acesso a comunicações móveis é diferenciado por gênero e é íntimo;
- um entendimento sobre cuidados em relação aos telefones celulares desde uma perspectiva de que eles são ferramentas ao mesmo tempo pessoais, públicas e privadas, e utilizadas para os movimentos;
- realizar trocas e praticar estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, colegas e nossos movimentos.

Para quem é esta atividade?

Pessoas que já pratiquem ou que estejam interessadas em *sexting* e que queiram discutir e praticar formas mais seguras de *sexting.*

Tempo estimado

Esta atividade requer cerca de **2 horas.**

> **Nota para facilitadora:** Este exercício leva cerca de 2,5 horas e nós recomendamos tomar algumas pausas durante o trabalho.

Recursos necessários para esta atividade

- Serviço de dados móveis
- Telefones celulares

Dinâmica

Em pares, discuta - 10 minutos

- Você já praticou *sexting?* Quando foi a primeira vez que você praticou *sexting?* O que você utilizou: telefones fixos, notas, cartas, cartões postais, bate-papo online?
- Como você usa seu telefone para praticar *sexting*? Aplicativos, mensagens de texto, fotos, vídeos, etc. O que você gosta, quais são os prós e os contras desta prática para você?
- Quais questões de segurança e privacidade você considera quando está praticando *sexting* e o que você faz para cuidar de sua segurança e privacidade?

Devolutiva com o grupo todo e trocas de estratégias - 35 minutos

Facilite as participantes a compartilharem o que é divertido e prazeroso a respeito de praticar *sexting* através de seus telefones.

> ***Marcadores de diferença:*** *existem estigmas em relação ao sexting e como as participantes de diferentes gêneros, sexualidades, raças, classes, idades, vivenciam este estigma de diferentes formas? Como as participantes lidam com a desaprovação social desta prática?*

Perguntas que você pode usar na discussão:

- Que tipos de mídia vocês gostam de usar e quais são os aplicativos que vocês mais gostam de usar? O que vocês mais gostam sobre esta prática? O que mais vocês gostariam de fazer com o aplicativo, com a mídia?
- Qual foi a coisa mais divertida que você já fez no sexting e por quê?

Troca de estratégias

Facilitadora, prepare pedaços grandes de papel com os seguintes títulos:

- Chegando a acordos
- O amor que fazemos, os dados que compartilhamos
- Aplicativos e cuidados básicos / considerações com dispositivos
- Carta Coringa

Facilite uma conversa a partir das questões-guia abaixo. Tome notas nos grandes papéis sobre as estratégias compartilhadas pelas participantes.

Chegando a acordos

- Faça acordos com parceires de *sexting* - que acordos você gostaria de fazer sobre como salvar, compartilhar digitalmente ou pessoalmente?
- Você já negociou acordos de sexting com parceires, como você faz isso?
- Rompimentos acontecem, como você negocia com seus parceires após um rompimento sobre sexting? Você mantém a sua palavra, será que o mesmo acontece do outro lado?

O amor que fazemos, os dados que compartilhamos

– informações que vão junto com as nossas fotos e as histórias que elas contam:

- Pense se você quer compartilhar fotos suas íntimas mostrando seu rosto

- Tente cobrir características físicas que possam te identificar como tatuagens, marcas de nascença etc.
- Use o editor de metadados Exif para limpar os metadados, tags de geolocalização e outras informações relevantes
- Use aplicativos com filtro *blur* para borrar seu rosto, tatuagens etc. (tipo Pixlr)

Aplicativos e cuidados básicos / considerações com dispositivos

- Escolha um aplicativo que ofereça recursos de privacidade e segurança como criptografia, deletar mensagens, e bloqueio de cópia da tela (*screenshot*)
- Use um aplicativo de mensagens seguro para práticas *sexting* para que você possa ter controle sobre as imagens e mensagens enviadas, de forma que você possa deletá-las se quiser
- *Nota de jargão: Autodestruição - O snapchat e outros aplicativos prometem "autodestruição", mas muitas vezes os conteúdos não são totalmente destruídos e as pessoas podem acessar as imagens para distribuição posterior.*
- Criptografe e coloque senha na tela inicial dos seus dispositivos
- Coloque senha nos seus aplicativos
- Considere o uso de um e-mail seguro e um número de telefone alternativo para as contas dos aplicativos utilizados
- Saiba como deletar e salvar
- Considere se o aplicativo está programado para fazer sincronização automática e se você quer que as práticas de *sexting* sejam sincronizadas e armazenadas

Mãos-na-massa: Aplicativos mais seguros e edição de imagens

Discussão sobre a escolha de aplicativos para *sexting*

Quais aplicativos as participantes estão usando para *sexting* e por quê? Quais precauções de segurança você toma ao escolher um aplicativo e quais os recursos de segurança que você gosta do aplicativo escolhido? Quais são as suas preocupações e receios?

Use aplicativos que sejam:

- Criptografados
- Protegidos por senha
- Não permitam salvar ou tirar cópias da tela (*screenshot)*
- Em que mensagens possam ser deletadas

> Avaliando SMS e MMS. SMS e MMS não oferecem estes recursos. Veja a atividade O que é um telefone? Como as comunicações móveis funcionam? para mais informações sobre SMS e MMS e vigilância.

Atividades mãos-na-massa

Facilitatora, esta atividade é uma oportunidade para as participantes praticarem estratégias de segurança recomendadas pelas facilitadoras que contribuíram com o FTX: Reiniciando com segurança. Selecione as atividades que acreditar serem mais relevantes para seu contexto. Algumas outras a serem consideradas:

- Criptografando e protegendo seus dispositivos com uma senha
- Removendo informações de identificação de fotos e dispositivos móveis
- Crie/configure um e-mail e número de telefone que sejam seguros

Partilhe essa lista de tarefas com as participantes e instrua-as a praticarem estas dicas em grupos pequenos, usando a si mesmas e a internet para responderem as perguntas que aparecerem.

Mãos-na-massa com imagens

- Pratique tirar fotos ocultando seu rosto
- Tente cobrir características físicas que possam te identificar como tatuagens, marcas de nascença etc.
- Use aplicativos com filtro *blur* para borrar seu rosto, tatuagens etc.

Mãos-na-massa com dispositivos e aplicativos

- Escolha e instale um aplicativo seguro
- Coloque senha nos seus aplicativos

- Saiba como deletar e salvar chats
- Saiba como deletar imagens de seus dispositivos

Devolutiva - 10 minutos

Como foi essa sessão para você?

- O que vocês fizeram?
- Incentive as participantes a compartilharem as mídias criadas, se elas quiserem.
- O que foi difícil, o que foi fácil? Com o que você ficou surpresa?
- Onde você procurou informações quando teve dúvidas?

Recursos adicionais

Oficina de *Sexting* das Luchadoras - momentos de *sexting* como conduzir, durante, depois. Armazenamento e compartilhamento, Mudança de consentimento e consentimento em todos esses momentos.

> **Notas da facilitadora:** Como excluir imagens de aplicativos e dispositivos é um pouco mais complicado, aqui estão algumas instruções específicas para ajudar as participantes a “Saber como excluir imagens do seu dispositivo” (última atualização em maio de 2019): Saber como excluir imagens do seu dispositivo requer o entendimento de como fazer isso na memória do seu aplicativo e também saber a localização de onde suas imagens são armazenadas no seu telefone celular. Em dispositivos IOS isso é mais opaco, pois você não tem acesso a arquivos além dos aplicativos onde os arquivos são criados. Isso também depende se você está ou não usando os aplicativos de bate-papo para tirar fotos ou se está preparando as fotos com antecedência (usando o aplicativo da câmera do celular).

Para usuárias do Telegram, clique no cabeçalho de uma conversa, em seguida, procure Fotos e Vídeos, você pode excluir imagens de lá. Isso excluirá as imagens do aplicativo Telegram, mas se você salvou essas imagens em outra pasta do dispositivo, terá que usar um gerenciador de arquivos para excluí-las. Você também pode ver e explorar arquivos compartilhados com uma usuária ou grupo específico.

No Signal, clique no cabeçalho de uma conversa. Você verá miniaturas de mídia compartilhada. Você pode excluir de lá. Novamente, isso excluirá apenas as imagens/mídia compartilhada no Signal, e se você salvou em outro lugar no seu dispositivo, haverá uma cópia lá. Isso também se aplica à pessoa com quem você estiver praticando *sexting*, ou seja, a pessoa também deve excluir.

Para usuários de Android, Usando um gerenciador de arquivos Removendo mídia e imagens no Telegram: vá para Armazenamento interno e procure a pasta Telegram >> Imagens do Telegram / Vídeo do Telegram / Documentos do Telegram / Áudio do Telegram. Em seguida, exclua os arquivos dessas pastas. Para o Signal, se você salvar uma imagem / mídia fora do Signal, poderá escolher onde salvá-la. Outros locais onde suas fotos / mídia podem estar: Armazenamento interno >> Fotos. Geralmente, você obterá diretórios (pastas) que armazenam suas fotos. Por padrão, as imagens salvas do Signal são salvas aí.

