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

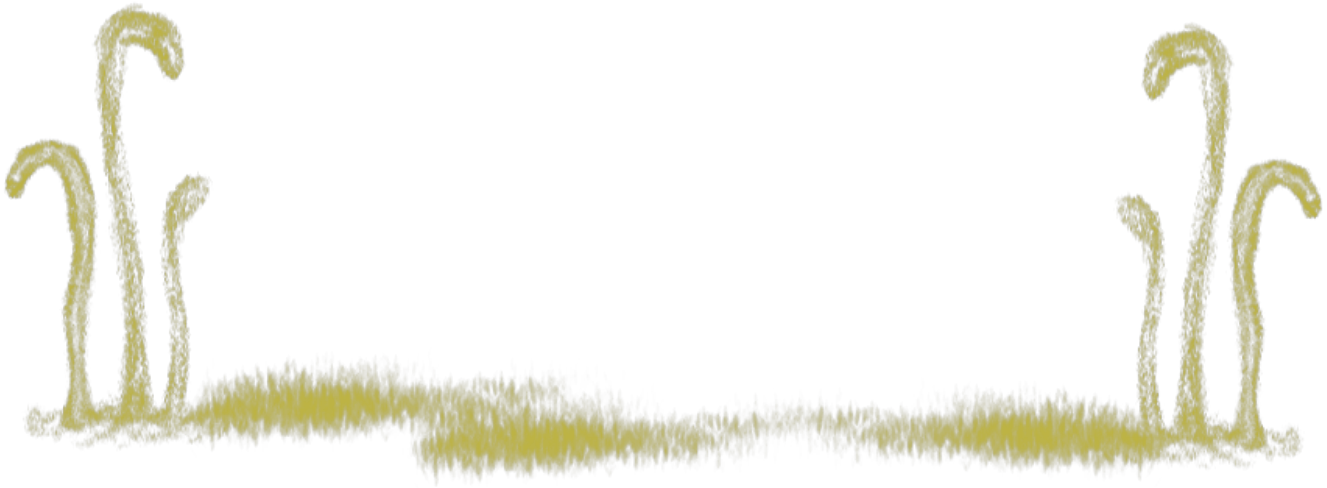
- Limpeza remota
- PixelKnot para mensagens criptografadas
- Briar para protestos e desligamentos de rede

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



Revision #3
Created 26 April 2023 01:41:55 by Kira
Updated 28 June 2023 20:58:06 by Kira