Image not found or type unknown

On a saisi mon téléphone! : Sauvegarde, verrouillage et suppression [activité tactique]

Cette activité vise à se préparer face à des situations où les participant·e·s et leurs téléphones seront en danger physiquement.

activ_tact_FR.png
Image not found or type unknown

Cette activité vise à se préparer face à des situations où les participant·e·s et leurs téléphones seront en danger physiquement. Voici quelques scénarios possibles :

- Risques lors de manifestations
- Risques lors de passages aux frontières
- Menaces d’arrestation ou de saisie du téléphone
- Risques de vol et de harcèlement

Cette activité se déroule en 4 étapes, incluant des activités pratiques facultatives de préparation des téléphones:

- Prendre soin de nous-mêmes : nos pratiques
- Préparer nos appareils en cas de risques
- Débriefing
- Complément d’informations (facultatif)

Si vous le désirez, cette activité peut être suivie d’exercices appliqués pour bien pratiquer les stratégies et tactiques de sûreté.

Objectifs d’apprentissage

- comprendre la sécurité mobile, en considérant les téléphones mobiles comme nos outils de communications personnelles, privées, publiques et militantes
- connaître les concepts de base du fonctionnement des communications mobiles pour mieux comprendre les risques liés à ces communications
- échanger et pratiquer des stratégies/tactiques en matière de sécurité mobile qui permettront de réduire les risques pour nous-mêmes, nos collègues, nos proches et nos mobilisations

À qui s’adresse cette activité ?

Cette activité peut être faite avec des participant·e·s ayant différents niveaux d’expérience d’utilisation stratégique et sécuritaire des téléphones mobiles. L’activité se penchera plus particulièrement sur le *care* et le bien-être.

Temps requis

Environ **1h20.**

Matériel

- Tableau blanc ou à feuilles mobiles ou grandes feuilles de papier (pour prendre en notes les discussions de groupe)
- Feuilles et crayons (pour l’exercice individuel)
- Marqueurs/feutres

Mécanique

Cet exercice est conçu pour accompagner des militant·e·s qui pourraient se trouver en situations risquées (manifestations, passages aux frontières, etc.) avec leurs téléphones mobiles. À la fin de cet exercice, iels auront un ensemble d'outils et de tactiques à leur disposition.

Prendre soin de nous-mêmes : nos pratiques - 20 minutes

> **Conseil care et bien-être :** Ceci est une activité tactique visant à se préparer face à des situations risquées et à préparer nos téléphones en conséquence. Prenez un moment pour reconnaître qu'avant de se préparer pour ce genre de situations, il faut d'abord connaître nos façons de prendre soin de nous-même.

Commencez par amener le groupe à discuter de leurs façons de prendre soin d'elleux-mêmes lors de situations à haut risque.

Demandez-leur de travailler individuellement. Donnez-leur du papier pour qu'iels écrivent leurs réponses. Voici les questions :

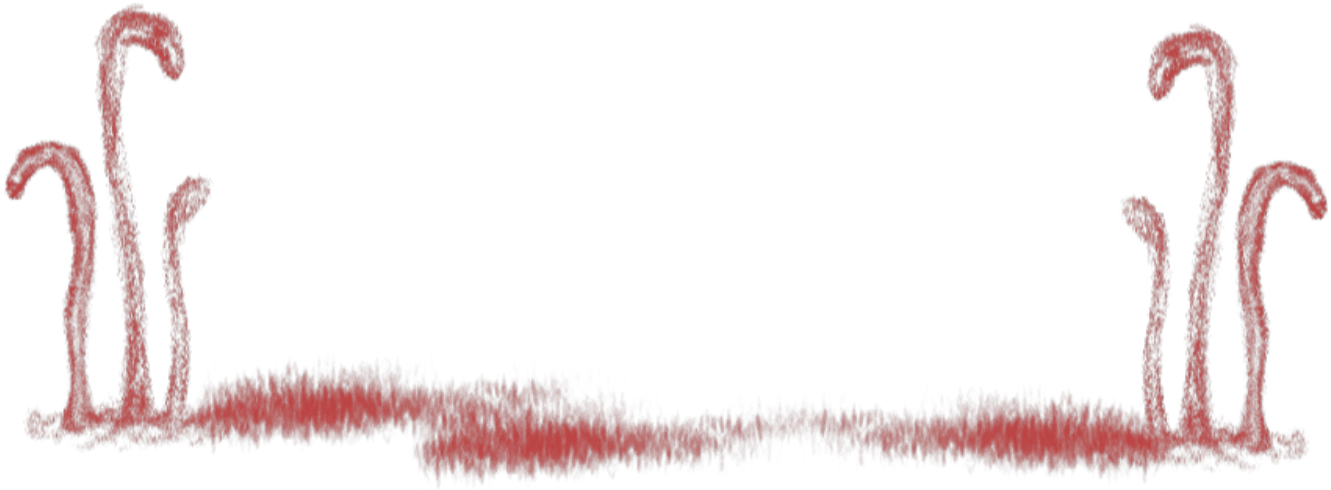
- Dans quel genre de situation avez-vous à réfléchir à votre sécurité physique et à celle de votre téléphone ?
- Que faites-vous déjà pour prendre soin de vous-même dans ces situations ? Pensez au avant, pendant et après.

Demandez-leur de diviser leur feuille en trois sections : avant, pendant et après. Leur feuille ressemblera à quelque chose comme ça :

	Exemple de feuille d’une participante	
AVANT	**PENDANT**	**APRÈS**

Puis, invitez les gens à partager avec le reste du groupe leurs pratiques d’autosoins et de bien-être. Ces pratiques peuvent être individuelles ou collectives. Écrivez leurs réponses sur un tableau blanc ou sur de grandes feuilles bien visibles pour tout le monde. Laissez-le dans un endroit bien visible.

Les participant·e·s utiliseront cette même méthode dans le prochain exercice.



Préparer nos appareils face aux risques - 30-45 minutes

Si vous travaillez avec un groupe qui se prépare pour un événement spécifique, il vaut mieux l'utiliser pour cet exercice. Les scénarios suivants ont été écrits pour les groupes qui ne se préparent pas à une situation spécifique. Nous vous invitons à les modifier au besoin.

Scénario 1 : Sécurité en manifestation

Vous vous apprêtez à participer à une manifestation. Vous voulez garder en sécurité les données de votre téléphone et vous voulez éviter d'être localisé·e et suivi·e pendant la manifestation. Malgré tout, vous voulez apporter votre téléphone pour pouvoir contacter des allié·e·s en cas d'urgence. Vous pensez également utiliser votre téléphone pour filmer la manifestation et les violations de droits humains qui auront lieu.

Scénario 2 : Risques lors de passages aux frontières

Vous êtes en déplacement et vous êtes sur le point de franchir une frontière vers une région dangereuse. Vous voulez pouvoir utiliser votre téléphone pour rester en contact avec vos allié·e·s, mais vous ne voulez pas que le téléphone serve à vous traquer. (Demandez au groupe quelles sont leurs stratégies dans les cas où une autre personne accède à leur téléphone. Exemples de ce type de situations : passages aux frontières, embarquement sur un vol, aller en manif.)

Scénario 3 : Menaces d’arrestation ou de saisie du téléphone

Vous avez appris par une source fiable que l’État menace de vous arrêter et de saisir vos appareils mobiles en raison de votre militantisme.

Scénario 4 : Risques de vol et de harcèlement

Vous craigniez qu’une personne vole votre téléphone et utilise son contenu pour vous harceler.

Demandez aux participant·e·s de former des équipes et demandez-leur de répondre aux questions suivantes. Les équipes devraient prendre des notes sur une grande feuille divisée en 3 (avant, pendant, après) comme présentée dans l’exercice individuel.

Les impacts sur les personnes : *Dans ce scénario (ou dans l’événement auquel vous vous préparez), quels sont les risques ? Quelles personnes sont touchées par ces risques ? Prenez en compte l’impact sur vous, les personnes qui sont dans votre téléphone d’une quelconque façon, vos luttes et mobilisations (si c’est votre cas).*

Les questions suivantes servent à guider vos participant·e·s vers une réduction stratégique des risques et des impacts sur les personnes.

Avant : Pensez à ce que vous pouvez faire pour préparer votre téléphone dans ce scénario.

- Quel genre de fichier allez-vous supprimer de votre téléphone ? Pourquoi ?
- Quelles applications allez-vous installer ? Pourquoi ?
- Qui sera informé·e de votre plan ? Pensez-vous aviser des personnes de votre situation avant et après l’événement ? Sera-t-il possible de le faire ?
- Quels sont les canaux de communications sécurisés que vous utiliserez ? Avec qui ?
- Avez-vous établi d’autres stratégies avec vos allié·e·s pour vous protéger pendant l’événement ?
- Localisation : Est-il plus sûr d’avoir l’option de localisation activée ou désactivée ? Voulez-vous que des personnes de confiance puissent vous localiser ?
- Effacement à distance : Voulez-vous activer l’option d’effacement à distance au cas où vous perdiez votre téléphone ?

Pendant : Pensez à comment vous utiliserez votre téléphone pendant le scénario.

- Batterie : Est-ce un souci ? Comment pouvez-vous vous assurer que vos appareils seront assez chargés ?
- Accès au réseau : Est-ce que cela pourrait poser problème ? Que ferez-vous si vous ne pouvez plus accéder à votre réseau mobile ? Avez-vous un plan en mode « hors ligne » ?
- Dans ce scénario, avec qui voulez-vous communiquer ? Comment pourrez-vous le faire ?
- Est-ce que vous êtes là pour filmer la manifestation ? Si oui, utiliserez-vous une application particulière pour le faire ?
- Qui pourra vous contacter sur votre téléphone mobile ?
- Avec qui communiquerez-vous avec votre téléphone ?
- Si vous décidez d'utiliser une nouvelle carte SIM pour cet événement, comment allez-vous choisir le fournisseur ? Est-ce qu'il en existe un plus sûr pour vos communications ? Qui pourra vous contacter à ce numéro ? Qui contacterez-vous ?

Après : Pensez à ce que vous ferez après le scénario.

- Images, audios, vidéos : Le cas échéant, que ferez-vous avec les médias que vous avez produits ?
- Métadonnées et traces laissées par votre appareil : Dans ce scénario, quelles sont les données produites par votre téléphone ? Pensez aux métadonnées, aux registres d'appels, à votre historique de localisation, etc.
- En cas de saisie de l'appareil : Comment saurez-vous si votre appareil est sur écoute ?
- En cas de vol ou de saisie : Que ferez-vous pour retrouver l'intégrité et la sécurité de votre téléphone mobile ?

Donnez-leur entre 30 et 45 minutes pour élaborer des plans, stratégies et tactiques.

Débriefing

Lorsque le temps est écoulé, demandez aux équipes de présenter leurs résultats.

Utilisez leurs comptes-rendus pour planifier vos exercices pratiques en sécurité mobile.

Complément d’informations – facultatif - 15 minutes

> **Conseil pour l’animation :** Tout dépendant de votre style d’animation ou de votre groupe, vous pouvez présenter ces compléments d’information pendant le débriefing ou dans une section informative. Voici des informations que nous estimons utiles pour vous aider à planifier votre atelier.

Avant

- **Communication de sûreté** : Informez des personnes que vous serez dans une situation où vous craigniez pour vous-même et vos biens. Avisez une personne de confiance de votre situation avant et après l’événement risqué. Déterminez à l’avance un rythme de communications avec cette personne, selon le niveau de risque de la situation.
- **Pour les situations à très haut risque :** Nous recommandons de contacter une personne désignée toutes les 10 minutes. Si par exemple, vous allez dans une manifestation très risquée ou que vous traversez une frontière dangereuse, prévoyez communiquer toutes les 10 minutes (si possible) pendant l’événement.
- **Pour les situations moins à risques :** Prenons un exemple. Vous êtes dans une ville pour un colloque avec des travailleuses du sexe et vous vous déplacez toute la journée pour vous rendre aux séances et réunions. Avisez votre partenaire de confiance de vos déplacements et de votre arrivée à chaque séance. Envoyez aussi un message quand vous allez au lit et quand vous commencez votre journée (ex. :« je me réveille »).
- **Nettoyez votre téléphone :** Quelles sont les choses que vous voulez garder confidentielles ?
- **Déconnexion :** Déconnectez-vous de toutes les applications dont vous n’aurez pas besoin. Si une personne prend possession de votre téléphone et que vous êtes connecté·e à des comptes, elle pourra y accéder, consulter vos historiques et les utiliser en votre nom.
- **Verrouillage et chiffrement :** Vous pouvez chiffrer votre téléphone, votre carte SD et votre carte SIM et attribuer un NIP pour chacune de ces choses. De cette façon, si une personne prend votre appareil, elle ne pourra pas accéder à vos informations ni l’utiliser sans vos codes. Dans le cas où on vous menacerait, vous ne pourrez peut-être pas

protéger vos mots de passe. Parlez-en avec vos camarades et prenez ceci en considération dans vos plans de sécurité.

- **Gare aux copies de votre appareil :** Plusieurs services de police ont des équipements qui permettent de copier des appareils électroniques (téléphones, portables, disques durs). Si votre téléphone est copié, la police pourra accéder à tout son contenu. Si vous chiffrez votre appareil, elle ne pourra pas y accéder sans votre mot de passe.
- **Silence :** Désactivez vos notifications (sonores et visuelles), utilisez le mode Silencieux.
- **Effacement à distance :** Vous pouvez décider d'activer l'option d'effacement à distance selon votre contexte. Dans certains cas, il est bien de vous assurer que vous pourrez (ou une personne de confiance) supprimer des contenus à distance si votre téléphone était perdu ou volé.
- **Cartes SIM et téléphones jetables :** Nos téléphones produisent et émettent beaucoup d'informations : nos messages, nos appels, les données envoyées aux applications ou notre localisation qui est fréquemment communiquée à nos opérateurs mobiles.
  - Demandez-vous si vous voulez apporter votre téléphone dans la situation risquée. Si oui, sachez que votre appareil est relié à votre identité et qu'il peut être suivi par vos opposants.
  - Pour éviter ce risque, vous pouvez laisser votre appareil à la maison et utiliser plutôt un téléphone jetable/prépayé. Vous devez l'utiliser pour cet événement seulement (le téléphone sera associé à l'événement) et vous devrez le jeter après coup.
  - Pour bien dissimuler votre identité, vous aurez besoin d'un téléphone jetable ET d'une nouvelle carte SIM. Nos téléphones ET nos cartes SIM contiennent une identité. Si vous mettez une nouvelle carte SIM dans votre téléphone régulier, vous serez encore identifiable par l'identité de votre appareil.
  - *Ceci est donc une option dispendieuse. Éviter d'être identifié·e par nos téléphones est une tâche qui demande beaucoup de planification. Pour que cela fonctionne, le téléphone de rechange devra vraiment être détruit. Si ce n'est pas possible de le jeter, vous pouvez avoir un téléphone alternatif que vous utilisez dans certaines situations. Toutefois, plus vous l'utilisez et plus il permettra de vous identifier.*
- **Enlever les cartes SIM :** Si vous vous retrouvez dans une situation risquée inattendue, vous voudrez peut-être enlever les parties qui contiennent des informations sensibles comme votre carte SIM et votre carte mémoire (si cela est possible). *Remarque : Dans certains cas, ceci est utilisé comme excuse par des agresseurs pour intensifier leur violence.*

Pendant

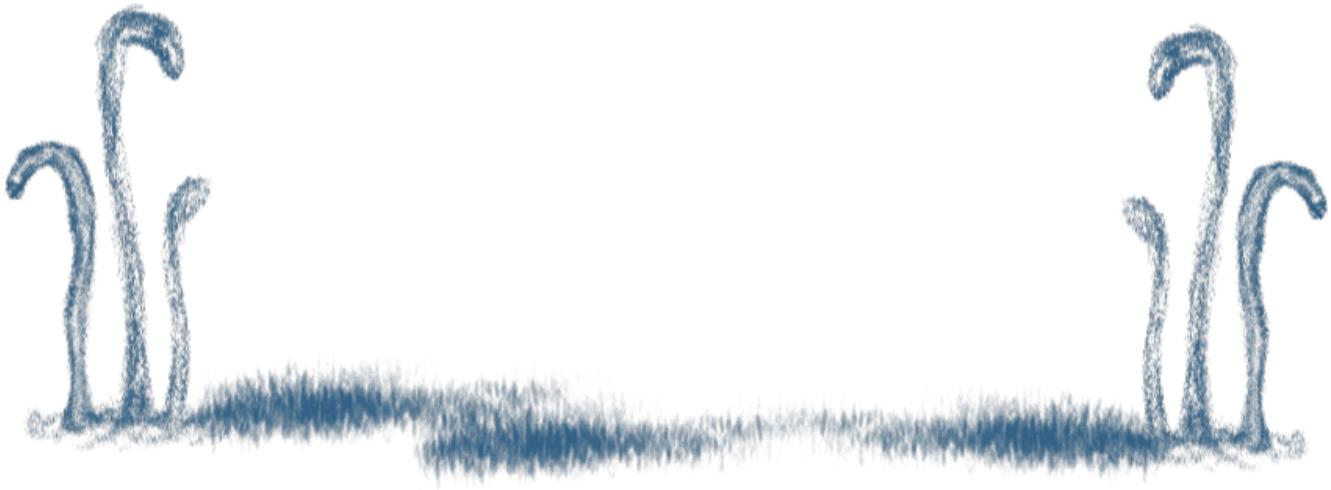
- Effacement à distance
- Application PixelKnot pour chiffrer vos messages (https://guardianproject.info/fr/apps/info.guardianproject.pixelknot/)
- Application Firechat pour les manifestations et les blocages de réseau

Après : On a confisqué ou fouillé votre téléphone ? Que faire ?

- **Nettoyez-le ou obtenez un nouveau téléphone :** Notre meilleur conseil est de réinitialiser les paramètres d'usine du téléphone. Si vous avez les moyens, achetez un nouvel appareil et faites analyser votre ancien téléphone (sans le réinitialiser).
- **Vos comptes et applications :** Réinitialiser tous vos mots de passe.
- **Dites-le autour de vous :** Si on vous a pris votre téléphone, faites-le savoir à vos contacts fréquents et parlez des impacts possibles sur ces personnes.

Ressources supplémentaires

- Guide pratique – chiffrer votre iPhone (EFF) : https://ssd.eff.org/fr/module/guide-pratique-chiffrer-votre-iphone
- Guide pratique – utiliser Signal pour iOS (EFF) : https://ssd.eff.org/fr/module/guide-pratique-utiliser-signal-pour-ios
- Guide pratique – utiliser Signal pour Android (EFF) : https://ssd.eff.org/fr/module/guide-pratique-utiliser-signal-pour-android
- Guide pratique – utiliser Whatsapp pour iOS (EFF) : https://ssd.eff.org/fr/module/guide-pratique-utiliser-whatsapp-pour-ios
- Guide pratique – utiliser Whatsapp pour Android (EFF) : https://ssd.eff.org/fr/module/guide-pratique-utiliser-whatsapp-pour-android



Revision #5

Created 26 April 2023 01:04:31 by Kira

Updated 28 June 2023 20:03:59 by Kira