Sécurité mobile

Élaborer des stratégies et tactiques pour que les participant·e·s puissent utiliser leurs téléphones mobiles de façon plus sécuritaire selon leurs propres contextes.

Introduction et objectifs d'apprentissage


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

Ce module vise à élaborer des stratégies et tactiques pour que les participant·e·s puissent utiliser leurs téléphones mobiles de façon plus sécuritaire selon leurs propres contextes.

Dans ce module, vous trouverez des conseils pour animer des discussions entourant l'accès aux technologies et communications mobiles pour les défenseur·e·s des droits des femmes et des droits sexuels/reproductifs. Ces discussions porteront sur l'accès différencié à ces technologies en fonction de notre genre ou de notre identité sexuelle. Nous discuterons de notre utilisation des téléphones mobiles pour nos communications privées/personnelles, pour nos communications publiques et pour notre activisme. Nous parlerons également de nos stratégies et de nos outils pour rendre nos communications mobiles plus sûres.

Dans ce module, vous trouverez : des activités de groupe pour analyser notre utilisation des téléphones mobiles en fonction de notre genre et de notre identité sexuelle; des activités pratiques pour explorer et comprendre comment fonctionnent les communications mobiles; des activités de groupe pour connaître et pratiquer des stratégies/tactiques rendant nos communications plus sûres; des guides d'animation vous permettant de faire le pont entre les questions de sécurité féministe et de sécurité mobile.

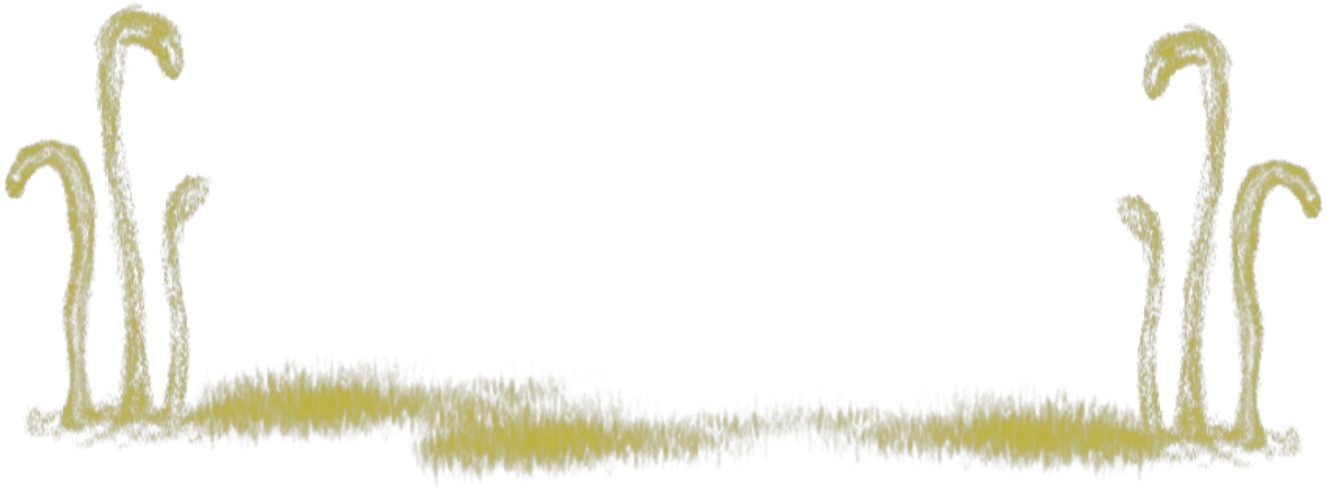
Voici des questionnements fréquents auxquels nous tentons de répondre dans ce module :

- Que se passe-t-il si une personne accède à mon téléphone ? Quel genre d'information se trouve sur mon téléphone ? Qu'est-ce qui pourrait m'arriver ? Qu'est-ce qui pourrait arriver à mes collègues, à mes camarades ou même à mon mouvement social ?
- Comment savoir si je suis surveillé·e par mon ou ma partenaire, par des ex, par des membres de ma famille ou par le gouvernement ?
- Comment puis-je utiliser mon téléphone de façon plus sûre ?
- Comment pouvons-nous utiliser nos téléphones pour nous organiser et nous mobiliser ?

Objectifs d'apprentissage

À la fin de ce module, les participant·e·s pourront :

- comprendre en quoi les communications mobiles et leur accès sont genrés et intimes
- 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 elleux-mêmes, leurs collègues, leurs proches et leurs mobilisations



Activités et parcours d'apprentissage

> **Cette page est essentielle** à la bonne utilisation et compréhension de ce module. En suivant les parcours d'apprentissage, cela permet aux participant·e·s de mieux appréhender les sujets étudiés.

Parcours d’apprentissage

Vous pouvez choisir une ou plusieurs activités pour votre formation. Nous recommandons de commencer par une activité d’introduction. Ceci permettra d’ouvrir une discussion avec les participant·e·s afin qu’iels **échangent sur leur expérience des téléphones mobiles** et en quoi celle-ci est influencée par le genre, la sexualité, la race, la classe, le handicap, etc.

Quelques recommandations spécifiques : Si votre groupe souhaite utiliser les téléphones mobiles **pour documenter la violence**, nous recommandons l’activité d’approfondissement Débat : Documenter la violence. Cette activité permettra de débattre et discuter des avantages et inconvénients liés à cette forme de documentation mobile. Nous recommandons ensuite l’activité tactique Documenter la violence : Planification et exercice pratique.

Pour les groupes qui désirent utiliser leurs téléphones **pour communiquer des actions, se mobiliser ou s’organiser** : nous recommandons les activités tactiques comme Actions et mobilisation : Planifier nos communications mobiles ou On a saisi mon téléphone ! : Sauvegarde, verrouillage et suppression.

Pour les participant·e·s qui utilisent leurs téléphones **pour faire des rencontres en ligne (applications de rencontres) ou pour sexter** : nous recommandons l’activité d’introduction Par ici vos téléphones et les activités tactiques Applis de rencontres, vie privée et sécurité et Sextos, plaisir et sécurité.

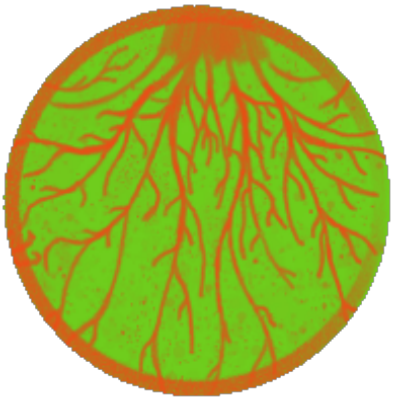
> **Conseil pour l'animation!** Il est fort probable que vos participant·e·s ne possèdent pas le même type de téléphone mobile. Vous pouvez former des petits groupes pendant les activités pratiques selon leur type de téléphone (iPhone, Android, téléphone mobile basique).

Activités d'apprentissage

Activités d’introduction

- Téléphones, intimité, sécurité et accès genré
- Ligne du temps téléphonique
- Randonnée de la sécurité mobile
- Par ici vos téléphones
- Mon téléphone et moi

Activités d'approfondissement



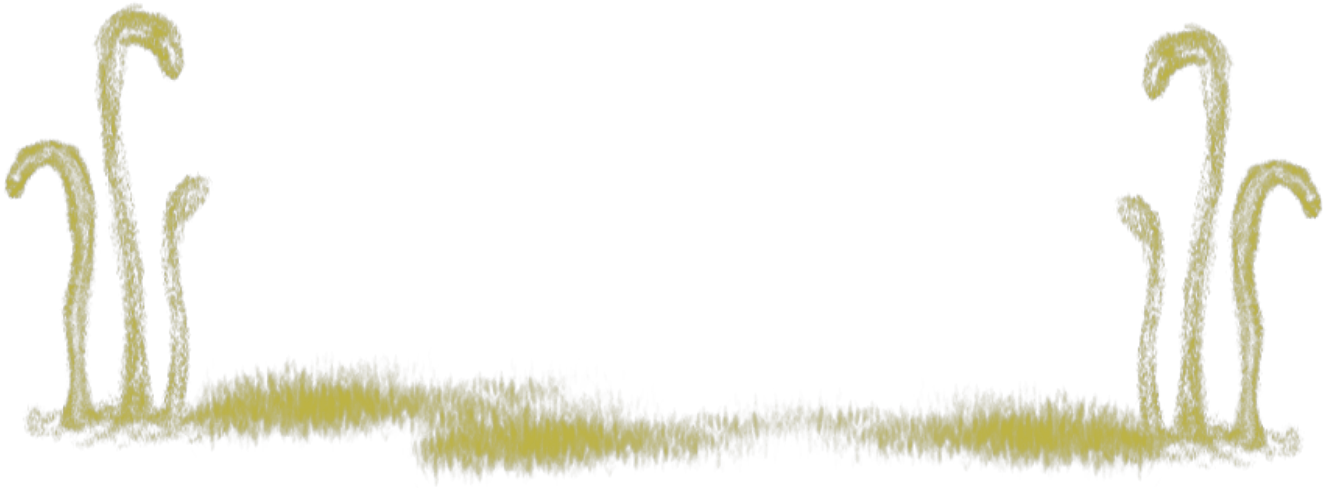
- Le pouvoir de la téléphonie mobile : Appareils, comptes, fournisseurs, État et politiques
- La téléphonie mobile : Comment ça marche ?
- Débat : Documenter la violence

Activités tactiques

- Actions et mobilisation : Planifier nos communications mobiles
- On a saisi mon téléphone ! : Sauvegarde, verrouillage et suppression
- Choisir nos applications mobiles
- Documenter la violence : Planification et exercice pratique
- Applis de rencontres, vie privée et sécurité
- Sextos, plaisir et sécurité

Ressources | Liens | Lectures

- Les guides de Video4Change (en anglais) : https://video4change.org/resource-categories/
- Les guides Witness (pour filmer et documenter les violations des droits humains) : https://fr.witness.org/
- Security in a Box - Outils et tactiques de sécurité numérique : https://securityinabox.org/fr/
- Les ressources de My Shadow « Prenez le contrôle de vos données »: https://myshadow.org/fr
- Le guide « Autodéfense contre la surveillance » de l'EFF : https://ssd.eff.org/fr



Téléphones, intimité, sécurité et accès genré [activité d'introduction]

activ-intro_FR.png
Image not found or type unknown

Cette activité permettra d'**amorcer une discussion** avec les participant·e·s sur leurs façons d'utiliser leurs téléphones. Vous pouvez utiliser cet exercice pour : présenter le concept de l'accès genré, souligner que nos différentes identités se manifestent dans l'espace mobile et pour souligner les risques et opportunités des communications mobiles.

Nous recommandons de faire cette activité en début de formation sur la sécurité mobile.

Cette activité se déroule en 3 étapes :

- Discussion en binôme
- Retour en grand groupe
- Synthèse de l'activité et des points communs par la personne animatrice

Objectif d'apprentissage

- comprendre en quoi les communications mobiles et leur accès sont genrés et intimes

À qui s'adresse cette activité?

N'importe qui utilisant ou ayant déjà utilisé un téléphone mobile.

Temps requis

Environ **30 minutes**

Matériel

- Un tableau blanc ou à feuilles mobiles

Mécanique

Nos téléphones mobiles sont le lieu de nos interactions intimes. Grâce à eux, nous sommes en contact avec nos proches, nos amoureuses·eux, nos ami·e·s. Nous faisons des appels, envoyons des messages, des images ou des vidéos plus ou moins intimes. De cette façon, nous comprenons nos téléphones mobiles comme des objets personnels et intimes. Toutefois, ils font aussi partie de quelque chose de plus grand : ils sont liés à des fournisseurs de télécommunications, ils sont régulés par des politiques gouvernementales, ils peuvent être confisqués, volés et scrutés sans notre consentement.

L'accès aux téléphones mobiles varie grandement en fonction du genre. Quand des femmes en utilisent, cela représente une remise en question du pouvoir : c'est pourquoi des gens s'attaquent aux femmes qui utilisent des téléphones. Dans certains contextes, des femmes peuvent les utiliser pour dénoncer des abus.

Discussion en binôme - 15 minutes

Demandez aux participant·e·s de former des équipes de deux. Ceci les encouragera à s'exprimer personnellement. À tour de rôle, une personne se confie pendant que l'autre écoute. Chaque personne a environ 5-7 minutes pour s'exprimer. Cela dépendra du temps qu'il faudra pour que les binômes se forment.

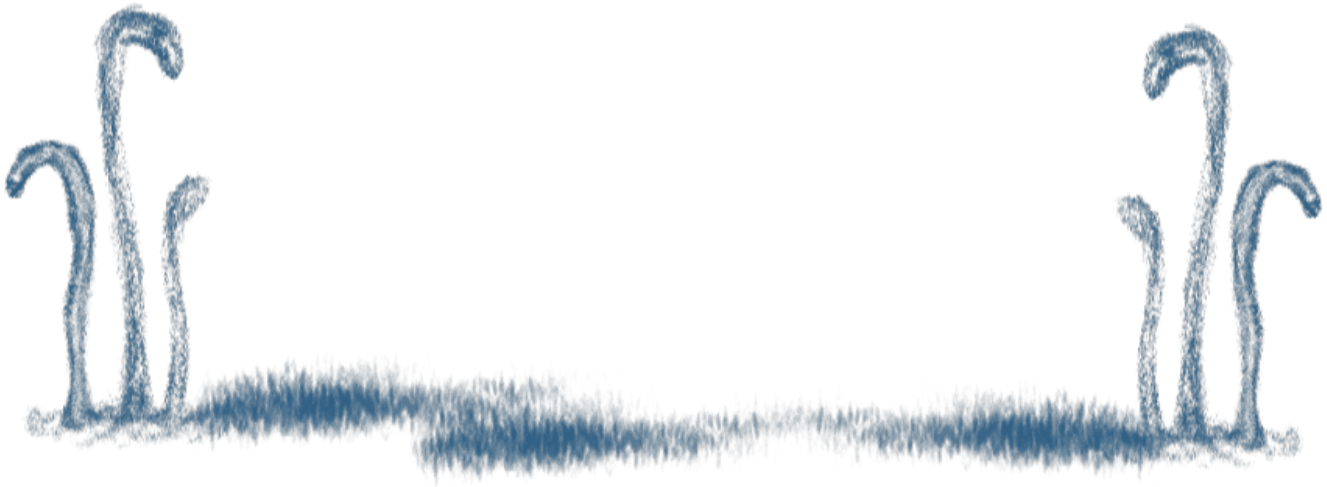
Questions

Écrivez-les à un endroit bien visible ou sur des bouts papier que vous donnez à chaque équipe.

- **Comment utilisez-vous votre téléphone ? Quand l'utilisez-vous ?** *Si les gens ne savent pas quoi répondre, demandez-leur comment ils l'utilisent avec différentes personnes comme leurs ami·e·s, leur famille, leurs collègues, des inconnu·e·s.*
- **Quand utilisez-vous votre téléphone pour faire de l'organisation et de la mobilisation ?**
- **À quels moments, vous ne vous sentez pas en sécurité en utilisant votre téléphone ? Que faites-vous dans ces situations ?** *Encouragez les participant·e·s à éviter les discussions sur le vol, et amenez-les plutôt vers des exemples comme : des colocataires, des partenaires ou des proches qui les surveillent, des confiscations par la police, etc.*

Retour en grand groupe - 15 minutes

Pendant que les binômes présentent leurs réponses au groupe, prenez des notes sur un tableau. Synthétisez leurs réponses. Y a-t-il des stratégies spécifiques que vous souhaitez aborder ? Ou encore des situations, des scénarios ?



Ligne du temps téléphonique [activité d'introdution]

ativ-intro_FR.png
Image not found or type unknown

Cette activité d’introduction invite les participant·e·s à échanger sur leurs expériences personnelles concernant leur téléphone mobile. L’activité les amènera à bouger et à raconter leur histoire. Iels pourront parler de leurs opinions respectives à l’égard des téléphones mobiles. Aussi, iels pourront parler de leurs façons personnelles, et significatives, d’utiliser leurs téléphones.

Cette activité est semblable au Mur de nos premières fois technologiques puisqu’elle invite les gens à partager leurs expériences personnelles des technologies mobiles et à les présenter sur une ligne du temps collective. Elle vous permettra de mieux connaître les expériences et les relations des participant·e·s avec les technologies mobiles.

Objectif d’apprentissage

comprendre en quoi les communications mobiles et leur accès sont genrés et intimes

À qui s’adresse cette activité?

N’importe qui utilisant ou ayant déjà utilisé un téléphone mobile.

Temps requis

Environ **30 minutes.**

Matériel

Des étiquettes pour identifier des périodes (de 5 ans) sur votre ligne du temps. Vous pouvez les écrire sur des feuilles de papier que vous déposez au sol (ex. : 1990, 1995, 2000, 2005, etc.).

Mécanique

Préparez une ligne du temps dans la pièce, au sol ou au mur.

Les participant·e·s devront se placer le long de la ligne du temps, en fonction de leurs réponses à vos questions. À la fin de chaque question, demandez quelles sont la première et la dernière date de la ligne. Si des petits groupes se sont formés sur la ligne, demandez-leur à quelle date ils se situent.

Vous pourrez leur poser deux questions ou plus, mais cela dépend de la taille du groupe et du temps dont vous disposez.

Pour les questions plus spécifiques (en italique), demandez à une ou deux personnes d'y répondre à voix haute.

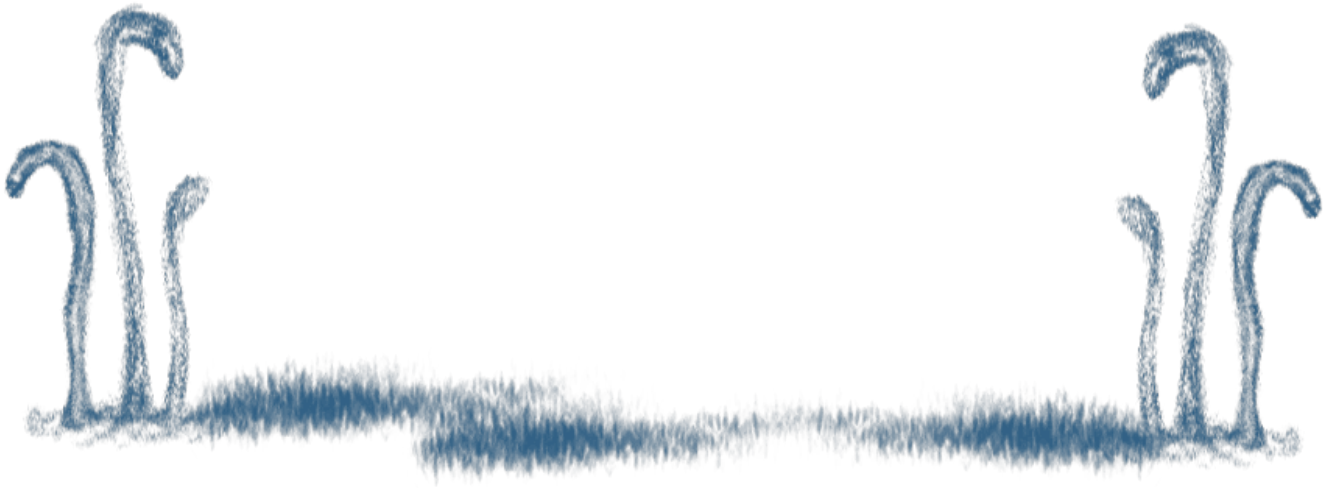
Voici les questions à poser

- **Quand avez-vous eu votre premier téléphone ?** *C'était comment ? L'avez-vous partagé avec d'autres personnes ? Quel âge aviez-vous ? Comment l'avez-vous utilisé ?*
- **Quand avez-vous eu votre premier téléphone intelligent ?** *Qu'est-ce que cela signifiait pour vous ? L'avez-vous partagé avec d'autres personnes ? Quelle est votre application préférée ? Et pourquoi ?*
- **Quand avez-vous utilisé l'internet pour la première fois avec votre téléphone ?** *Quel site web avez-vous consulté en premier ? Et pourquoi ?*
- **Quand avez-vous cessé d'utiliser un téléphone pour la première fois ?** *Qu'est-ce que vous avez conservé de ce téléphone (ex.: photos, textos, mémoire) ? Et pourquoi ?*

Débriefing - 5-10 minutes

Demandez aux participant·e·s si iels ont des observations ou des commentaires à faire à propos de l'exercice. Résumez leurs réponses et faites des liens avec les questions d'intimité et d'accès genré. Prenez en compte le rapport qu'iels ont avec leurs téléphones et leurs façons préférées de les utiliser.

> **Remarque sur l'intersectionnalité :** Dans votre groupe, est-ce que l'accès aux téléphones mobiles varie en fonction du genre, de la sexualité, de la race ou de la classe ? Si oui, comment ? Qu'en est-il de leur vie privée sur leurs téléphones ?



Randonnée de la sécurité mobile [activité d'introduction]

ativ-intro_FR.png
Image not found or type unknown

Cette activité d’introduction vise à sensibiliser les participant·e·s aux questions de sécurité mobile. L’activité vous permet de connaître les mesures de sécurité déjà prises par les participant·e·s et de voir les risques/vulnérabilités qui pourraient être traités en priorité. Nous recommandons de faire ceci en début de formation sur la sécurité mobile.

Objectif d’apprentissage

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 ?

N’importe qui utilisant ou ayant déjà utilisé un téléphone mobile.

Temps requis

Environ **30 minutes.**

Mécanique

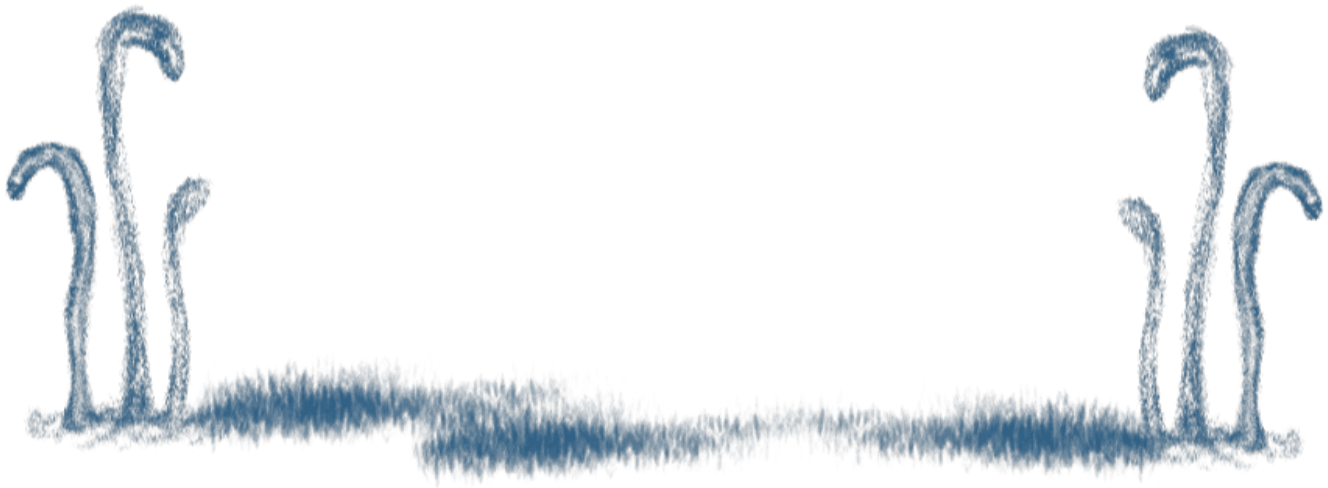
Demandez aux participant·e·s de se mettre en ligne, côte à côte. Posez-leur des questions à propos de la sécurité mobile. Les participant·e·s doivent faire un pas en avant si leur réponse est « oui » et faire un pas en arrière si la réponse est « non ».

Exemples de questions

- Est-ce que vous avez un écran de verrouillage ?
- Est-ce vous verrouillez vos applications ?
- Est-ce que vous avez une carte SIM non enregistrée ?
- Est-ce que vous avez un courriel alternatif pour votre téléphone ? (Un autre que votre courriel principal)
- Est-ce que vous avez activé la fonction « Localiser mon appareil » sur votre téléphone ?
- Est-ce que la localisation est activée sur votre téléphone ?
- Est-ce que vous avez une copie du contenu de votre téléphone ? (photos, messages, vidéos, etc.)
- Est-ce que vous avez un antivirus sur votre téléphone ?

Débriefing - 5-10 minutes

Demandez aux participant·e·s si iels ont des observations ou des commentaires à faire à propos de l’exercice. Synthétisez le tout et faites des liens entre cette randonnée et l’ordre du jour de votre formation.



Par ici vos téléphones [activité d'introduction]

ativ-intro_FR.png
Image not found or type unknown

Cette activité d’introduction a pour objectif de faire ressortir les émotions qu’on ressent face à nos appareils mobiles et lorsque d’autres personnes les saisissent et/ou accèdent à leur contenu.

Objectifs d’apprentissage

- comprendre en quoi les communications mobiles et leur accès sont genrés et intimes
- comprendre la sécurité mobile, en considérant les téléphones mobiles comme nos outils de communications personnelles, privées, publiques et militantes

À qui s’adresse cette activité ?

Cette activité fonctionne particulièrement bien avec les groupes subissant souvent des formes de confiscation de leurs appareils (par la police, des partenaires, la famille, etc.). Nous la recommandons pour les groupes souhaitant discuter des impacts qu’ils subissent et de leurs réactions émotionnelles face à ces confiscations.

> **Conseil *care* et bien-être :** Nous recommandons de faire cette activité avec grand **soin** et avec respect. Les participant·e·s doivent pouvoir y donner un **consentement** libre et éclairé. Cette activité risque de mieux fonctionner si vous avez développé un **lien de confiance** avec votre groupe.

> **Remarque à propos des parcours d’apprentissage :** C’est une très bonne activité d’introduction qui préparera votre groupe aux discussions et aux activités tactiques qui abordent les situations à haut risque (comme la perte ou le vol de téléphones).

Temps requis

Environ **30 minutes.**

Mécanique

Activité : Ramassez les téléphones des participant·e·s - 15 minutes

Ramassez les téléphones des participant·e·s (avec leur consentement clair et explicite), mais sans leur expliquer pourquoi vous le faites.

Discussion

Demandez-leur :

- Comment vous sentez-vous sans votre téléphone dans vos mains ?
- Qu’est-ce que vous ressentez sur le coup ?

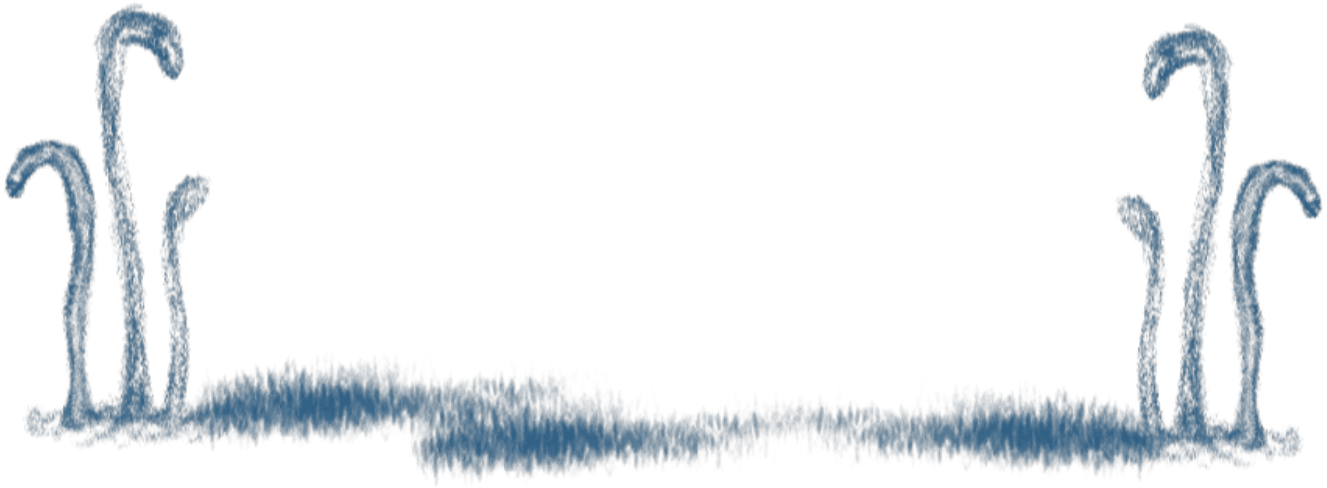
Activité : Redonnez les téléphones et débriefing - 5-10 minutes

Vous pouvez maintenant leur redonner leurs téléphones.

Discussion

Demandez-leur :

- Qu’est-ce que vous avez ressenti en perdant votre téléphone ? Pourquoi ?
- Comment vous sentez-vous d’avoir retrouvé votre téléphone ? Pourquoi ?
- Est-ce qu’on vous enlève parfois votre téléphone ? Qui vous l’enlève et dans quel contexte ?
- Comment vous sentez-vous quand on vous l’enlève ? Pourquoi ?
- Pourquoi votre téléphone est-il important pour vous ? À quoi votre téléphone vous permet-il d’accéder ? *Encouragez-les à être précis·e·s par rapport à leur relation avec leur téléphone, sur son importance et sur les choses auxquelles il leur permet de se connecter.*



Mon téléphone et moi [Activité d'introduction]

ativ-intro_FR.png
Image not found or type unknown

Cette **activité d’introduction** a été conçue pour être très rapide. Elle invite les participant·e·s à réfléchir à leur utilisation des téléphones mobiles et en quoi celle-ci est intime de plusieurs façons. L’activité permettra au groupe d’échanger leurs stratégies et leurs préoccupations liées à la surveillance et à la vie privée sur téléphone mobile.

Nous recommandons de faire cette activité en début de formation sur la sécurité mobile.

Objectif d’apprentissage

comprendre en quoi les communications mobiles et leur accès sont genrés et intimes

À qui s’adresse cette activité ?

N’importe qui utilisant ou ayant déjà utilisé un téléphone mobile.

Temps requis

Environ **30 minutes.**

Matériel

- Un tableau blanc ou à feuilles mobiles

Mécanique

Discussions en binôme - 15 minutes

Demandez aux participant·e·s de former des équipes de deux. Ceci les encouragera à s'exprimer personnellement. À tour de rôle, une personne se confie pendant que l'autre écoute. Chaque personne a environ 5-7 minutes pour s'exprimer. Cela dépendra du temps qu'il faudra pour que les binômes se forment. Voici les questions :

Question 1 : Quelles sont les choses les plus personnelles et les plus intimes que vous faites sur votre téléphone ?

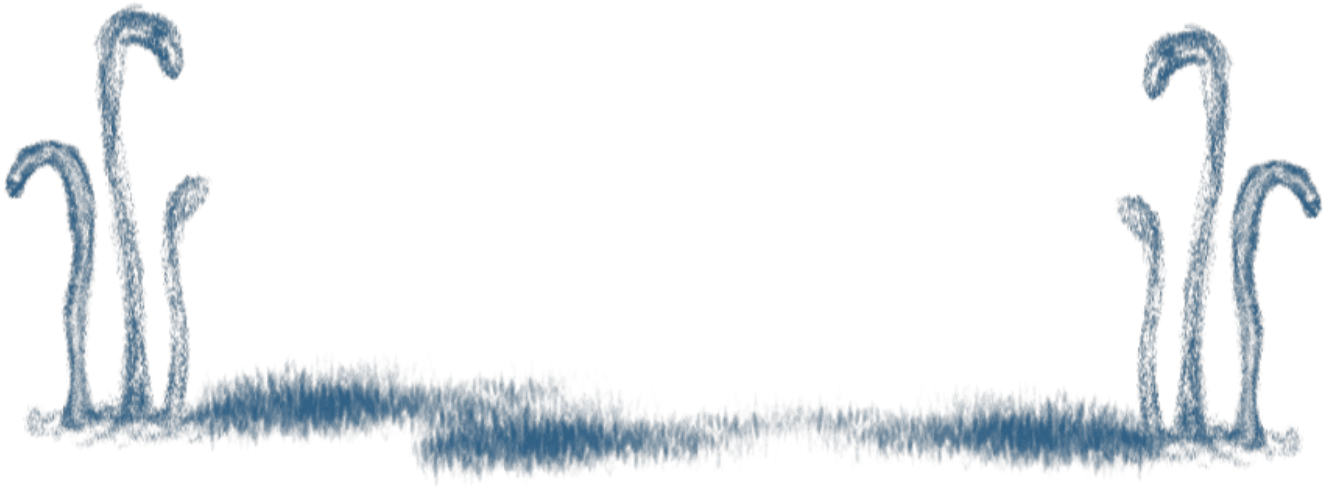
Question 2 : Qu'est-ce que vous faites pour prendre soin de ces communications/contenus/expériences intimes ?

Donnez-leur un ou deux exemples de réponses personnelles de votre cru pour les inspirer. Exemples : des selfies nus que vous faites pour le plaisir ou pour vous exprimer, des sextos ou des conversations intimes que vous avez avec d'autres, etc.

> **Remarque sur l'intersectionnalité :** Dans votre groupe, est-ce que l'accès aux téléphones mobiles varie en fonction du genre, de la sexualité, de la race, de la classe ou du handicap ? Si oui, comment ? Qu'en est-il de leur vie privée ?

Retour en grand groupe - 15 minutes

Rassemblez le groupe et demandez aux binômes de présenter leurs réponses. Pendant ce temps, prenez des notes (au tableau, si désiré) pour synthétiser le tout ensuite. Faites ressortir les points communs de leurs discussions. Voici quelques questions à vous poser pour guider votre synthèse : Comment les gens utilisent-ils leurs téléphones ? Et en quoi est-ce intime ? Est-ce que les participant·e·s ont mentionné que leur genre affectait leur accès aux téléphones mobiles ? Ou que cela affectait leur vie privée ? Qu'est-ce qu'iels font pour prendre soin de leurs communications intimes (interactions, images, vidéos, messages, etc.) ? Quelles sont leurs préoccupations ? Est-ce qu'iels font des liens entre la vie privée et le genre, la sexualité, la race, la classe, le handicap, l'âge ? Si oui, lesquels ?



Le pouvoir de la téléphonie mobile : Appareils, comptes, fournisseurs, état et politiques [activité d'approfondissement]

activ_aprof_FR.png
Image not found or type unknown

Dans cette activité, les participant·e·s seront amené·e·s à **créer collectivement un schéma conceptuel**. Iels discuteront de leur rapport à leurs téléphones, à leurs comptes de services mobiles et à leurs fournisseurs de téléphonie mobile. Dans une moindre mesure, iels discuteront de la manière dont les politiques gouvernementales et les politiques d'entreprises entrent en jeu dans ce rapport.

Nous recommandons de faire cette activité en début de formation sur la sécurité mobile.

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

À qui s'adresse cette activité ?

N'importe qui utilisant ou ayant déjà utilisé un téléphone mobile.

Temps requis

Environ **45 minutes.** Si vous souhaitez aborder son contenu plus rapidement, vous pouvez poser moins de questions au groupe et leur présenter plutôt un exemple de schéma conceptuel.

Matériel

- Tableau à feuilles mobiles
- Marqueurs/feutres

Mécanique

Posez une série de questions au groupe et dessinez au tableau un schéma à partir de leurs réponses. L'objectif est d'essayer de schématiser les relations des participant·e·s avec leurs téléphones mobiles. Iels discuteront du pouvoir de la téléphonie mobile, de contrôle et d'autonomie en examinant leurs relations avec **leurs appareils, leurs comptes, leurs fournisseurs et les politiques gouvernementales et d'entreprises.**

Suggestions pour la préparation

- Renseignez-vous sur les fournisseurs de téléphonie mobile dans la région ;
- Renseignez-vous sur les liens entre ces fournisseurs et l'État (est-ce que ce sont des fournisseurs/opérateurs gérés par l'État ?) ;
- Préparez quelques exemples locaux de militant·e·s féministes (droits des femmes, droits sexuels, etc.) qui utilisent des téléphones mobiles pour leur activisme : expliquez en quoi cela est lié au pouvoir et de quelle façon les entreprises et/ou l'État réagissent/réglementent (si c'est le cas).

Pendant que vous posez les questions au groupe, **dessinez au tableau un schéma conceptuel** à un endroit bien visible pour tout le groupe.

> **Remarque :** Sur votre schéma, indiquez les choix/décisions qui ont été imposés aux participant·e·s (ex. : le type de téléphone, le nombre de personnes qui peut y accéder, la façon de choisir le téléphone, le fournisseur de téléphone mobile, le type de plan/forfait et qui peut y accéder)

Voici de quoi pourrait avoir l'air un schéma :

mobile-screenshot.png
Image not found or type unknown

Questions à poser au groupe

- **À propos des appareils :** Quel genre de téléphone utilisez-vous ? Comment l'avez-vous obtenu ? Est-ce que vous le partagez avec d'autres personnes ? Si oui, comment et avec qui ?
- **À propos de votre fournisseur mobile :** Comment avez-vous sélectionné votre fournisseur ? Est-ce que vous partagez votre forfait/plan avec d'autres personnes ? Est-ce vous qui gérez votre propre forfait ? Si non, qui le gère ? Est-ce que vous avez choisi votre forfait ? Comment l'avez-vous choisi ?

Discussion

La relation entre nous et nos fournisseurs mobiles. Avez-vous signé les conditions générales d'utilisation ? Qu'avez-vous accepté en signant votre contrat ? Qu'est-ce que votre fournisseur a accepté ?

> **Conseil pour l'animation :** Si vous êtes au courant de problèmes particuliers avec des fournisseurs mobiles de la région, essayez d'apporter leurs conditions générales d'utilisation en exemple. Donnez aussi des exemples de cas où des utilisateurs·trices ont interpellé ces fournisseurs sur des questions de sécurité.

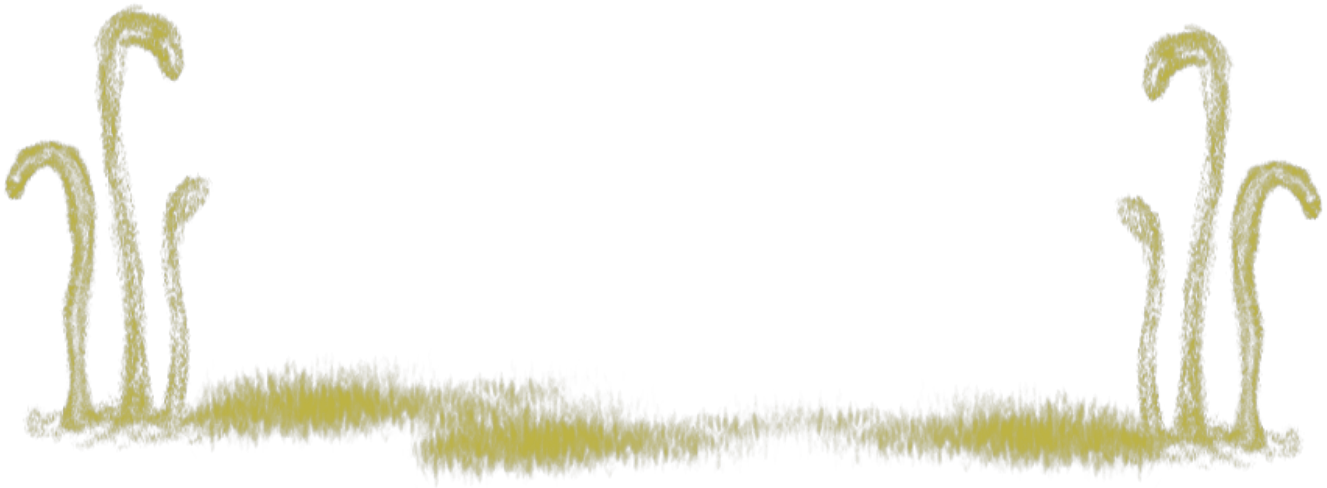
Discussion

La relation entre les fournisseurs mobiles et l'État. Les fournisseurs sont-ils gérés par l'État ? Est-ce que ce sont des compagnies locales, régionales ou internationales ?

> **Conseil pour l'animation :** Pour vous préparer, il est conseillé de faire des recherches sur l'influence ou les régulations de l'État sur la téléphonie mobile. Y a-t-il eu des cas récents de blocage des services mobiles par l'État ? Est-ce que les participant·e·s sont habitué·e·s aux blocages de services ciblant des individus ? Est-ce que les forces de sécurité procèdent à des saisies d'appareils mobiles ?

Ressources supplémentaires

- Études de cas : *N'hésitez pas à trouver des études de cas adaptées à votre groupe et à leur contexte.*
- Une lise des opérateurs de télécommunications à travers le monde (Wikipédia) : https://fr.wikipedia.org/wiki/Liste_des_op%C3%A9rateurs_de_t%C3%A9l%C3%A9communications
- Enregistrement des cartes SIM 101 (en anglais) : https://privacyinternational.org/explainer/2654/101-sim-card-registration



La téléphonie mobile : Comment ça marche ? [activité d'approfondissement]

ativ_aprof_FR.png
image not found or type unknown

Le but de cette activité est d’approfondir les connaissances des participant·e·s sur le fonctionnement des communications mobiles. L’objectif est d’accroître leur capacité à évaluer/planifier les risques des communications mobiles. Cette activité est *essentielle* à votre formation en sécurité mobile. Si vous ne l’incluez pas dans votre programme, assurez-vous que les participant·e·s connaissent déjà les notions présentées dans cette activité. Cette activité permet de maîtriser les bases en évaluation des risques techniques de la téléphonie mobile.

Cette activité se déroule en 2 étapes :

- Dissection de téléphones
- Présentation : Les données de communications mobiles et les risques associés

Objectif d’apprentissage

- connaître les concepts de base du fonctionnement des communications mobiles pour mieux comprendre les risques liés à ces communications

À qui s’adresse cette activité ?

N’importe quelle personne qui participe à une formation sur la sécurité mobile.

Temps requis

Environ **45 minutes.**

Matériel

- Quelques téléphones mobiles que vous pourrez ouvrir et examiner
- Un tableau, une diapositive ou des feuilles avec les informations principales écrites dessus

Mécanique

Mentionnez que cette activité servira à parler des technologies mobiles : tout appareil électronique facile à transporter/qui se met bien dans une poche, qui permet de communiquer (appels et textos, accès internet et données mobiles). Certaines sections s'appliquent aussi les tablettes.

Disséquer nos téléphones - 5 minutes

Prenez un téléphone et ouvrez-le. Rappelez au groupe que notre téléphone est comme un petit ordinateur.

Demandez à tout le monde d'ouvrir son téléphone et d'identifier :

- Les parties qui servent à écouter ou projeter du son (micro, haut-parleurs)
- Les parties qui peuvent « regarder » et afficher des images (caméra, écran)
- Les parties qui envoient et reçoivent de l'information externe (GPS, antenne, wifi)
- Les parties semblables à un ordinateur (batterie, circuits électroniques, disque dur)
- Mémoire (cartes SD, autre mémoire intégrée au téléphone)
- Les cartes SIM

Présentation : L'appareil et son identité SIM - 5 minutes

Les téléphones sont composés de plusieurs petites pièces et ils contiennent quelques éléments d'identification. En plus de la marque, du modèle et du système d'exploitation, les téléphones portent deux noms : un identifiant d'appareil et un identifiant de carte SIM. Il est important de les connaître, car ils peuvent permettre de nous identifier. Il faut savoir notre téléphone communique régulièrement ces informations (en particulier le IMSI).

- **IMEI = nom de votre appareil**

Pour en savoir plus sur l'IMEI (International Mobile Equipment Identifier) :

https://fr.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- **IMSI = nom de votre carte SIM**

Pour en savoir plus sur l'IMSI (International Mobile Subscriber Identity)

https://fr.wikipedia.org/wiki/International_Mobile_Subscriber_Identity

Présentation : Ce que nos téléphones communiquent - 35 minutes

Nous utilisons nos téléphones pour communiquer avec les gens : par SMS, par messagerie, par les réseaux sociaux, des applications et les appels. Nos téléphones communiquent aussi de l'information sur eux-mêmes et sur NOUS : comme nos messages, mais aussi nos métadonnées, notre localisation, etc. Ces informations peuvent être reliées à d'autres informations personnelles comme nos réseaux sociaux, nos réseaux de militantisme, nos habitudes, notre lieu de travail.

C'est une bonne chose d'en avoir conscience, car cela nous permet de comprendre de quelles façons nos téléphones servent à nous suivre quotidiennement. Ceci crée un historique de nos déplacements et activités.

1. Votre téléphone est bavard

Votre téléphone communique différemment avec plusieurs types de réseaux pour annoncer qu'il est proche, pour se connecter ou vérifier si quelqu'un·e veut se connecter.

Opérateurs de téléphonie mobile

Ils ont des tours et des antennes avec lesquelles votre téléphone communique. Chaque antenne est désignée à une région spécifique. Votre téléphone s'enregistre auprès de la ou des tours les plus proches. Il **donne toujours votre IMSI** pour annoncer quel opérateur mobile vous utilisez et votre numéro afin que vous puissiez recevoir des messages, des appels et des communications sur votre appareil. Chaque fois que vous êtes près d'une tour, c'est comme si vous mettiez un point précisément daté et identifié sur une carte. Vous marquez l'endroit où vous vous trouvez, le moment où vous y êtes et ce que vous faites à cet endroit en termes d'utilisation de votre téléphone.

GPS

Si votre GPS est activé, votre téléphone est en train de communiquer avec les satellites GPS, et comme mentionné plus haut, ceci revient à placer un point précisément daté/identifié sur une carte.

Wifi

Si votre wifi est activé, votre téléphone tentera de se connecter aux réseaux Wifi qu'il croise. Il laisse ainsi une marque sur ces réseaux et il pourrait enregistrer le nom des réseaux dans votre téléphone.

Bluetooth ou NFC (Near Field Communication)

Si ces options sont activées, d'autres appareils utilisant le Bluetooth ou NFC pourraient communiquer avec votre appareil, pourraient tenter de se connecter ou de partager des fichiers, etc.

Discutez avec le groupe

Lesquelles de ces options doivent être activées et à quel moment ? Est-ce que les historiques de vos déplacements représentent un risque pour vous ?

2. Vous parlez beaucoup aussi

Nous utilisons nos téléphones pour communiquer. Il existe différents types de communications et leurs fonctionnements diffèrent (que ce soit pour l'émission ou la réception des messages).

SMS

Les SMS (messages textes et métadonnées) qui sont envoyés, puis stockés sur votre appareil et auprès de votre opérateur, sont toujours transmis « en clair » (cleartext, en anglais). Pour faire une métaphore, les SMS sont comme des cartes postales. Si une personne les intercepte, elle pourra les lire entièrement ainsi que connaître ses métadonnées (l'expéditeur, le destinataire, l'heure, la date).

MMS (messagerie multimédia)

Les MMS, c'est-à-dire les messages multimédias et leurs métadonnées, peuvent être chiffrés ou non. Si une personne tente d'en intercepter, il est possible qu'elle puisse les voir – cela dépend de leur chiffrement. Une fois envoyé, le message apparaîtra dans l'historique de votre fournisseur mobile et celui de votre destinataire. En cas d'enquête, ceci pourrait révéler les métadonnées (l'expéditeur, le destinataire, l'heure, la date) et le contenu du message.

Appels

Normalement, le contenu des appels est chiffré lorsqu'ils sont en cours. Toutefois, votre opérateur mobile, ou celui de votre destinataire, enregistrent les métadonnées de l'appel (l'expéditeur, le destinataire, l'heure, la date). Si un adversaire politique a accès à votre opérateur mobile, il pourrait écouter les appels et les enregistrer.

> Pour plus d'informations à propos des applications de messagerie, consultez l'activité Choisir nos applications mobiles.

Remarque sur la surveillance étatique : La surveillance étatique varie d'un pays à l'autre. À certains endroits, les gouvernements peuvent accéder à toutes les données des opérateurs mobiles. Dans ces cas-ci, il faut considérer que toutes nos métadonnées et nos contenus de services/applications non-chiffrés sont accessibles au gouvernement à tout moment (en temps réel ou après-coup s'il y a une enquête). **Le meilleur moyen de défense contre la surveillance est le chiffrement bout-en-bout.**

3. Votre téléphone est un petit ordinateur

Les logiciels malveillants : Votre téléphone peut être infecté par un virus ou un malware tout comme un ordinateur. Certaines personnes et certains gouvernements utilisent des logiciels pour mettre des appareils mobiles sous écoute. Ce genre de logiciel se sert souvent d'une partie du téléphone comme outil de traçage ou de surveillance (ex. : écoute par le microphone, suivre la localisation de l'appareil).

4. Le nuage/cloud est comme un classeur

Nos téléphones accèdent à certaines données qui se trouvent dans le nuage (aussi appelé le « cloud »). En gros, le « nuage » c'est un mot pour désigner l'internet. Des données sont stockées sur des serveurs physiques et ces serveurs sont connectés à l'internet. Les applications sur nos téléphones peuvent donc accéder à des données sur le nuage qui, en fait, ne sont pas vraiment sur notre appareil.

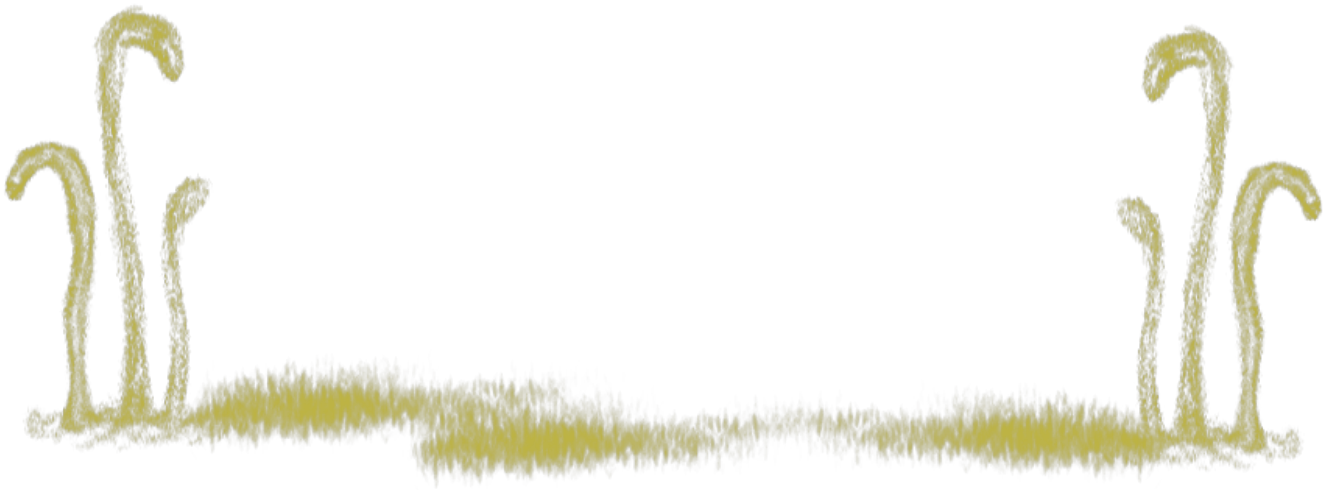
Quelques considérations : Est-ce que mon service mobile ou mon application chiffrent mes données en transit ? Est-ce que mes données sont chiffrées une fois stockées par le service mobile ? Est-ce que j'ai connaissances de situations où des opposants politiques ont pu accéder à ce genre de données ? Si oui, quand et comment ?

Conseil pour l'animation : Pendant que vous présentez toutes ces informations, il est fort probable que les participant·e·s posent des questions sur les pièces des appareils, sur les risques associés aux différents types de communications, etc. Prenez le temps d'y répondre. Si possible, faites une liste de leurs questionnements et des sujets qui sont à approfondir. Vous pourriez les écrire sur un tableau blanc, par exemple. Faites aussi une liste des questions et sujets que vous n'aborderez pas dans cette activité. Vous pourrez y revenir plus tard dans votre formation ou leur suggérer un suivi informatif post-formation.

Ressources supplémentaires

- WikiHow: Comment trouver l'identifiant IMEI sur un téléphone: https://fr.wikihow.com/trouver-l%E2%80%99identifiant-IMEI-sur-un-t%C3%A9l%C3%A9phone

- Comment trouver son code IMEI, et à quoi sert-il ? (en anglais):
  https://www.echosdunet.net/dossiers/code-imei
- Pour en savoir plus sur l'IMEI (International Mobile Equipment Identifier) :
- https://fr.wikipedia.org/wiki/International_Mobile_Equipment_Identity
- Pour en savoir plus sur l'IMSI (International Mobile Subscriber Identity)
  https://fr.wikipedia.org/wiki/International_Mobile_Subscriber_Identity
- Comment fonctionne l'internet et les communications mobiles (Guide MyShadow de TactitalTech) :
  https://myshadow.org/ckeditor_assets/attachments/267/fr_howtheinternetworks.pdf
- Ressources du site My Shadow (Tactital Tech), quelques unes sont en français :
  https://myshadow.org/materials



Débat : Documenter la violence [activité d'approfondissement]

ativ_aprof_FR.png
Image not found or type unknown

Dans cette activité d’approfondissement, vous animerez une **discussion** sur l’utilisation des téléphones mobiles pour documenter des violences et de quelle manière ceci peut perpétuer les violences. Dans cet exercice, vous pourrez discuter de cas particuliers de médias activistes/militants qui souhaitaient dénoncer et mettre fin à des violences en les documentant (enregistrer, filmer, photographier), mais qui ont eu pour conséquences de reproduire les violences .

Les participant·e·s pourront parler de leurs façons d’utiliser les téléphones pour documenter des violences. Iels pourront débattre et discuter des conséquences de la publication de ces images en ligne.

Objectif d’apprentissage

- comprendre la sécurité mobile, en considérant les téléphones mobiles comme nos outils de communications personnelles, privées, publiques et militantes

À qui s’adresse cette activité ?

Les groupes qui utilisent ou qui songent à utiliser leurs téléphones mobiles pour documenter des violences.

Temps requis

Environ **60 minutes.**

Matériel

- Des études de cas imprimées ou des liens vers des études de cas.

Mécanique

En grand groupe - 10 minutes

Demandez aux participant·e·s de parler de leurs expériences d'utilisation des téléphones mobiles pour documenter des violences.

> **Conseil *care* et bien-être :** Les gens vont donner des exemples qui pourraient les bouleverser ainsi que d'autres personnes du groupe. Prenez le temps de mentionner les ententes communes de votre atelier en matière de discussions portant sur la violence. Vous pourriez prendre un moment pour avertir que des actes de violence seront mentionnés pendant cet exercice. Rappelez à tout le monde d'écouter leurs limites quand iels racontent leur histoire ou leurs exemples. Invitez-les à prendre soin d'elleux-mêmes quand iels se sentent bouleversé·e·s et à arrêter de parler quand iels en ressentent le besoin.

Questions pour le groupe:

- Est-ce que le fait de filmer/enregistrer/photographier des violences – et de publier ces images ou enregistrements – a déjà eu des impacts positifs sur votre communauté ? Sur votre travail ? Sur vos luttes de défense de droits ? Pouvez-vous nous donner des exemples ?
- Qu'est-ce que vous documentiez ?
- Que s'est-il passé ?
- Comment avez-vous publié ces preuves (audios, vidéos, photos) ?
- Avec qui les avez-vous partagées ? Comment aviez-vous choisi ces personnes ?
- Quelle fut leur réponse ?

> **Conseil pour l'animation :** Vous pourriez préparer des exemples récents de mouvements locaux ayant utilisé des téléphones pour documenter des violences. Demandez aux participant·e·s de parler de leurs expériences en ce sens. Exemples : documenter (filmer, enregistrer, photographier) les violences de l'État, transférer des vidéos d'actes de violence, diffuser en direct des violences, les risques qui viennent avec le fait de posséder ce genre d'images, etc.

Vous trouverez des exemples dans la section **Ressources supplémentaires** plus bas. Vous pouvez utiliser ces exemples de cas pour la prochaine étape de l'activité qui est le travail en petits groupes. Vous pouvez aussi choisir d'autres cas qui vous semblent plus appropriés et plus récents pour votre groupe.

Expliquez que le but de l’activité est de créer un espace de débats et de discussions sur cet enjeu.

Études de cas en petits groupes - 20 minutes

Donnez un scénario à chaque petit groupe pour qu’iels le lisent et en discutent. Vous trouverez les scénarios un peu plus bas. Vous pouvez les modifier, en écrire ou en choisir d’autres plus appropriés pour votre groupe.

Questions pour les discussions en petits groupes :

- Dans ce scénario, comment utilise-t-on les téléphones mobiles pour documenter la violence ?
- Par rapport à ce scénario, donnez des arguments en faveur de l’utilisation des téléphones pour documenter la violence.
- Par rapport à ce scénario, donnez des arguments contre l’utilisation des téléphones pour documenter la violence.
- Dans cet exemple, de quelles façons pourrait-on réduire les conséquences négatives de l’utilisation des téléphones pour filmer/enregistrer/documenter des violences ?

Les scénarios

Les scénarios suivants pourront vous inspirer dans l’écriture de vos propres scénarios adaptés à vos participant·e·s. Écrivez-en plus qu’un, car cela vous permettra d’aborder plusieurs enjeux avec votre groupe. Les exemples suivants sont conçus pour déclencher des discussions reliant l’usage des téléphones mobiles (pour documenter des violences) aux mouvements sociaux, au consentement, aux conséquences possibles et à la reproduction de la violence.

Scénario 1

Votre communauté et vous faites face à du harcèlement et des violences. Avec d’autres personnes, vous vous organisez pour filmer des actes de violence et pour ensuite publier les vidéos sur les réseaux sociaux. Vous y ajoutez des sous-titres et du texte qui explique la situation et le contexte de violences. Dans votre publication, vous ajoutez aussi la liste des revendications de votre communauté ainsi que des ressources pouvant soutenir les personnes victimes de ces violences.

Scénario 2

Vous êtes témoin d’un acte de violence dans la rue et vous commencez à le diffuser en direct sur votre compte Facebook. Vous avez des milliers d’abonné·e·s sur votre compte. Vous ne connaissez pas la personne que vous filmez et vous ne connaissez pas le contexte.

Scénario 3

Depuis quelque temps, vous faites partie d'un groupe qui diffuse en direct des manifestations dans le but de montrer la force de ces actions, mais aussi pour documenter les violences subies par les manifestant·e·s. Vous apprenez que vos images sont utilisées par la police et par des adversaires politiques pour cibler des manifestant·e·s. Des images sont aussi utilisées et modifiées pour créer des vidéos hostiles aux manifestant·e·s qui sont diffusées sur les réseaux sociaux.

Retour en grand groupe - 30 minutes

Ce retour en grand groupe donne l'occasion aux équipes de présenter leur étude de cas et leurs arguments. Vous animerez alors une discussion de groupe sur les défis que pose l'enregistrement par téléphone de violences et leurs diffusions en ligne. Donnez assez de temps aux équipes pour faire leur compte-rendu et pour que le reste du groupe puisse réagir.

Pour la discussion de groupe :

- Quel était votre scénario ?
- Quels étaient les arguments pour et contre l'utilisation des téléphones pour documenter des violences ?
- Cela soulève quel(s) problème(s) ? Avez-vous déjà rencontré ce(s) problème(s) ? Qu'est-ce que vous en pensez ? Comment pouvez-vous agir stratégiquement pour obtenir le meilleur impact possible ? Qu'est-ce que vous pouvez faire pour réduire le plus possible les impacts négatifs ?

Pendant que les participant·e·s font leurs comptes-rendus et discutent, faites ressortir les points communs. Portez un regard attentif aux principales préoccupations de votre groupe. Vous pourriez animer une présentation ou un atelier sur ces questions plus tard. *Exemples de préoccupations techniques ou stratégiques :* comment documenter/enregistrer/filmer, stocker et publier ; comment vérifier l'authenticité des images/vidéos/audios (enjeu des deepfakes) ; comment la publication d'images peut inciter à la violence ; comment la diffusion ou le partage d'images violentes peuvent reproduire la violence, etc.

Ressources supplémentaires

Études de cas, articles de blog et articles journalistiques sur le sujet

> **Remarque :** Nous vous recommandons de trouver des exemples de cas locaux ou qui seraient plus pertinents pour votre groupe. Pour mieux vous préparer, demandez en amont des exemples à vos participant·e·s ou à l'organisation qui accueille votre formation. Vous

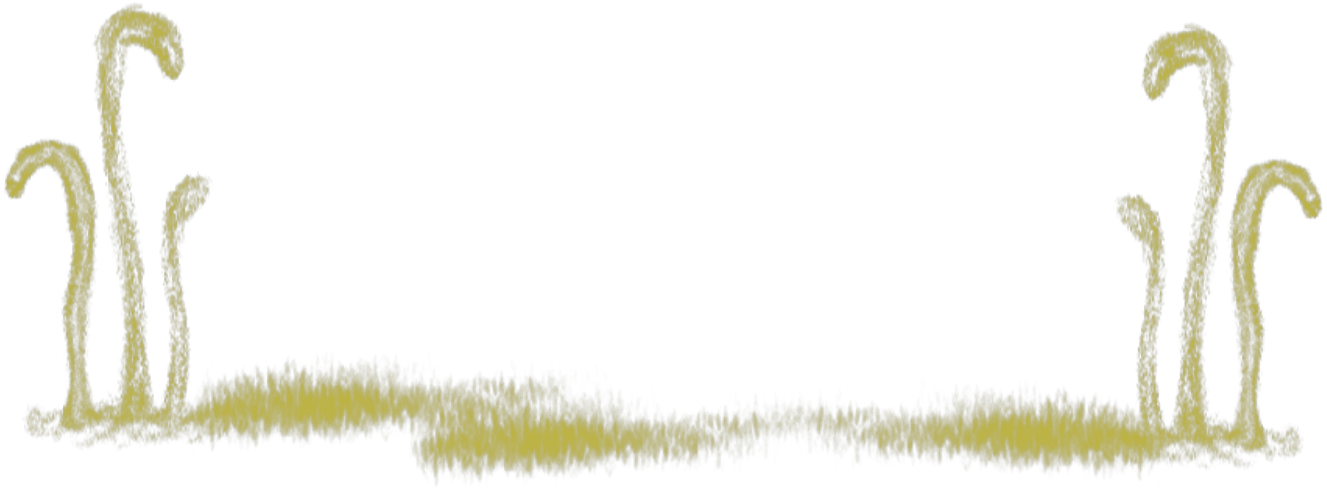
pouvez aussi trouver des articles qui questionnent le fait de diffuser en ligne des violences pour les dénoncer ou documenter.

- **« Une image, mille mots et des baffes qui se perdent »** : Dans cet article du collectif afroféministe Cases Rebelles, on critique le partage d'images violentes et retraumatisantes. « Qu'il s'agisse de meurtres policiers, de vieux crimes coloniaux, de guerres, de violences post-électorales, ces images concernent systématiquement des corps non-blancs à qui l'on refuse la dignité et l'intimité jusqu'au bout. » : http://www.cases-rebelles.org/une-image-mille-mots-et-des-baffes-qui-se-perdent/

« De l'usage des caméras en manifestation » : https://lundi.am/De-l-usage-des-cameras-en-manifestation

Les exemples suivants sont en anglais :

- Le Centre for Migrant Advocacy aux **Philippines** documente les abus subis par les travailleurs et travailleuses migrant·e·s : https://centerformigrantadvocacy.com/2016/10/26/ofw-sos/
- Étude de cas sur la diffusion en direct d'actes violents (tuerie de Christchurch) : « Les enjeux éthiques de la diffusion en direct sur internet » : https://mediaengagement.org/research/matters-of-facebook-live-or-death/
- « The world is turning against live streaming. » Article sur la tuerie de Christchurch (Nouvelle-Zélande) et comment l'**Australie** lutte contre la diffusion en direct de vidéos violentes non filtrées https://www.theverge.com/interface/2019/4/4/18294951/australia-live-streaming-law-facebook-twitter-periscope
- **Brésil** : « 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/
- Violence sur Whatsapp en **Inde** : « Suite aux violences en Inde et au Myanmar, Whatsapp réduira les limites de transferts pour lutter contre la diffusion de fausses nouvelles » https://www.vox.com/2018/7/19/17594156/whatsapp-limit-forwarding-fake-news-violence-india-myanmar
- Le cas du C-SPAN aux **États-Unis** : Des membres du Congrès américain diffusent en direct leur sit-in pour demander un vote sur la législation du contrôle des armes à feu. https://www.politico.com/story/2016/06/cspan-house-sitin-democrats-224696



Actions et mobilisation : Planifier nos communications mobiles [activité tactique]

activ_tact_FR.png
image not found or type unknown

Cette activité vise à guider les groupes qui souhaitent organiser ou participer à des actions en utilisant des applications de messageries. Les discussions que vous animerez permettront aux groupes de réfléchir à leurs différents types de communications. Elles leur permettront aussi d'élaborer des protocoles collectifs de sécurité en matière d'administration de groupes, de messages et d'appareils mobiles. Iels pourront adapter ces protocoles en fonction de leurs types de communications.

Cette activité se déroule en 4 étapes :

- Cartographier nos communications et évaluer les risques
- Planification : Créer un groupe de messagerie et ses paramètres
- Installation d'application (facultatif)
- Implantation (facultatif)

Si votre groupe n'a pas choisi l'application de messagerie qui leur convient, vous pourriez d'abord faire l'activité Choisir nos applications mobiles.

Objectif d'apprentissage

- 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 des téléphones mobiles. Si certain·e·s participant·e·s prévoient gérer des groupes de messagerie, prévoyez intégrer l'étape 4 de l'atelier qui vise l'implantation d'un groupe.

Temps requis

Environ **1 heure** pour les étapes 1 et 2. Environ **3 heures** si vous décidez de faire aussi les étapes 3 et 4.

Matériel

- Des feuilles de papier pour dessiner leur cartographie

Mécanique

1. Cartographier nos communications et évaluer les risques

Considérations sur la vie privée

Prenez en considération que vous communiquez différents types de messages sur l'application Signal et que certains messages sont moins privés que d'autres. Cartographier le genre de communications que vous avez et formez des groupes de messagerie qui correspondent à vos besoins en matière de vie privée et confidentialité.

Quels sont vos différents types de communications ? Selon leurs différents types, qui devrait avoir accès à ces communications ? *Suggérez aux participant·e·s de prendre en considération ces différents groupes de personnes. Demandez-leur si certain·e·s possèdent plus d'informations que d'autres. Ex. : Est-ce qu'il y a une information qui devrait être connue par seulement deux personnes ? Est-ce qu'il y a une information qui devrait être connue par une seule personne et qui ne devrait pas être partagée avec d'autres ? Est-ce qu'une information devrait être documentée et jamais diffusée ?*

Cette information :	**Exemples de communications :**
Doit être connue par un groupe de confiance très restreint	La localisation des organisatrices

Est essentielle et doit être connue par les bénévoles ou des petits groupes pour pouvoir se coordonner	La localisation changeante de la foule
Peut être partagée publiquement	L'heure du rassemblement, les groupes qui endossent publiquement l'action

Planification : Créer un groupe de messagerie et ses paramètres

Travaillez avec les participant·e·s pour les aider à concevoir des groupes de messagerie qui correspondent à leurs différents types de communications.

Suggestions pour guider la création de groupes: *Nous vous suggérons de commencer par utiliser ces questions-guides. Nous avons également inclus des suggestions de modèles de groupes fréquents. Demandez-leur de réfléchir à ce qui fonctionnerait ou non dans leur cas. Invitez-les à modifier ces paramètres en fonction de leurs besoins.*

Membres

- QUI ? – Qui peut se joindre au groupe ?
- COMMENT ? – Comment les gens peuvent-ils se joindre au groupe ? Y a-t-il une procédure ? Doivent-ils être vérifiés et approuvés, être présentés ? Doivent-ils accepter une invitation ou faire une demande d'inscription ?
- RECONNAISSANCE – De quelle façon votre groupe prend-il le temps de reconnaître l'arrivée d'une nouvelle personne ? Est-ce que votre groupe désire faire ceci ? Si oui, pourquoi ? Et si non, pourquoi ?
- RESPECT DES RÈGLES – Que faites-vous si une personne se joint sans suivre la procédure ?
- INFORMATIONS PERSONNELLES – Selon l'application de messagerie que vous utilisez, est-ce que les membres peuvent voir les numéros des autres personnes ? Si tel est le cas, toute personne qui a besoin que son numéro ne soit pas connu dans le cadre de l'action ne doit pas se joindre à un grand groupe où les autres personnes ne connaissent pas déjà son numéro et son implication dans l'organisation.

VÉRIFICATION – Sachez à qui vous parlez

Pour un type de communication donné, comment allez-vous vérifier la personne avec qui vous communiquez ?

- FACE À FACE – Est-ce que vous voulez exiger que chaque nouvelle personne doive rencontrer le groupe en personne pour devenir membre ? Est-ce qu'une personne peut être ajoutée si elle est approuvée par un·e membre ?
- NUMÉROS DE VÉRIFICATION – Vérifiez que vos messages se rendent sur les bons appareils. Si vous utilisez Signal ou Whatsapp, vérifier vos numéros de sécurité.

- MOTS DE SÉCURITÉ – Vérifiez que vos appels se rendent aux bons appareils. Si vous utilisez Signal pour vous appeler, DITES VOS MOTS DE SÉCURITÉ. Si vous utilisez une autre application, voulez-vous mettre en place un code entre vous pour vérifier que vous parlez à la bonne personne et qu'elle peut le faire librement ?

Sécurité des messages : Paramètres

Selon la nature des informations que vous communiquez, entendez-vous sur les paramètres de messages à utiliser dans le groupe.

- SUPPRIMER des messages – Les membres du groupe devraient conserver les conversations sur leurs appareils pendant combien de temps ?
- Messages ÉPHÉMÈRES – Dans une discussion Signal, vous pouvez activer l'option des messages éphémères et décidez après combien de temps des messages sont supprimés. Voulez-vous utiliser cette option ? De quelle façon et pourquoi ?
- CACHER les messages sur votre écran d'accueil – Réglez les paramètres de vos applications de messagerie afin que vos notifications ne soient pas visibles sur votre écran d'accueil. De cette façon, si vous perdez votre téléphone, les personnes ne pourront pas lire les messages qui apparaissent sur votre écran d'accueil.
- CODES – Pour les informations extrêmement sensibles, nous vous suggérons d'établir des mots de code avant votre action. Par exemple, vous pourriez dire « On est prêtes pour l'heure du thé ! » plutôt que « On est prêtes pour la manif ! ».

Modèles suggérés de groupes fréquents

1. Très petit groupe, avec des personnes vérifiées, pour des informations sensibles

> **Risque :** Que des personnes inconnues ou non-désirées se joignent au groupe et aient accès à des informations confidentielles.

- Lorsque vous disposez d'informations sensibles qui ne doivent être communiquées qu'à un petit groupe de personnes connues ;
- Très petit groupe, 8 ou moins, tout le monde se connaît et s'est rencontré en personnes ;
- Ajoutez les nouvelles personnes au groupe seulement quand vous êtes physiquement avec elles ;
- VÉRIFIEZ vos identités (vos numéros de sécurité sur Signal, par exemple) en personnes ;
- Si les numéros de sécurité d'une personne changent, revérifiez vos # en personnes ;
- Ne communiquez jamais plus que ce qui est nécessaire, ne prenez pas de risques inutiles ;
- SUPPRIMEZ

2. Les cellules / petits groupes

> **Risque :** Que des personnes vont joindre le groupe et y partager des informations inutiles ou volontairement incorrectes.

- Ce type de groupe permet d'éviter que des individus viennent spammer le grand groupe, le rendant inutilisable et trop bruyant ;
- 2 à 20 personnes : dans l'optique de limiter le bavardage inutile. Ayez un nombre gérable de cellules ;
- Un grand groupe peut avoir plusieurs cellules pour que la communication reste gérable et pertinente ;
- Les cellules sont connectées entre elles afin que les informations puissent y circuler. Vous pourriez envisager d'avoir une personne-ressource dans chaque cellule afin qu'elle puisse transmettre les informations dont tout le monde a besoin ;

3. Groupe public, information publique

Vous devez considérer que les informations transmises dans ce groupe sont publiques, et ce en temps réel. Bien que les informations de tous les types de groupes pourraient être divulguées publiquement, vous devez considérer ce type de groupe comme entièrement public.

- Pour toutes les informations que vous voulez partager publiquement, utilisez ce genre de groupe !

Sécurité de votre appareil

Si on vous vole votre téléphone, empêchez des intrus de se faire passer pour vous, de lire vos informations comme vos messages, vos contacts, vos courriels, etc. Pour des conseils d'animation plus détaillés sur la sécurité des appareils, voir l'activité : On a saisi mon téléphone ! : Sauvegarde, verrouillage et suppression.

- Réglez votre verrouillage afin de la déclencher avec n'importe quel bouton ;
- Choisissez un mot de passe fort ;
- Chiffrez votre téléphone ;
- Chiffrez votre carte SIM.

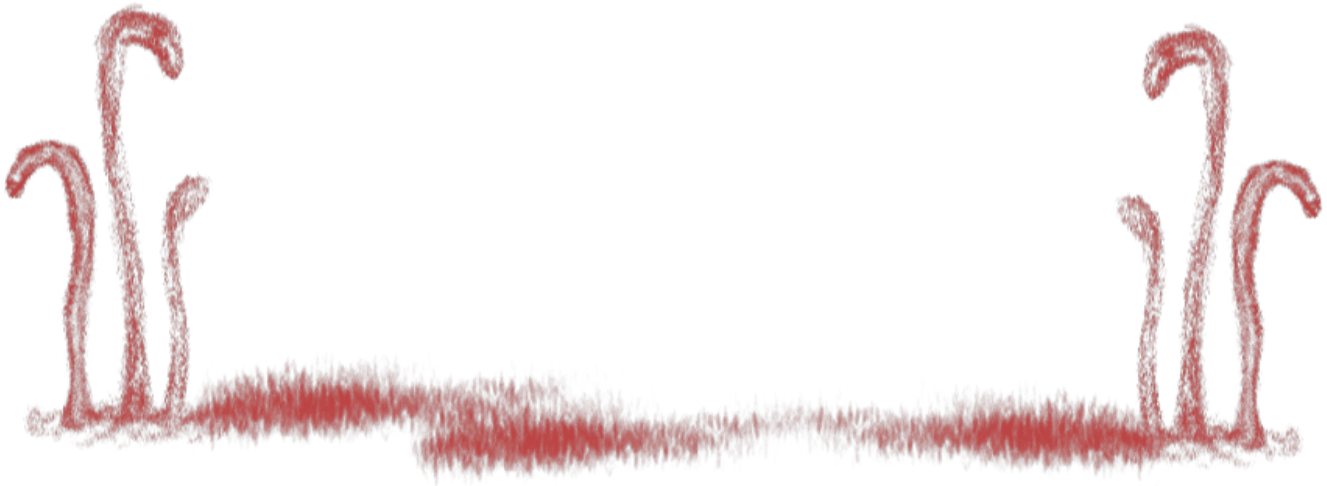
Batterie et réseau

Que faire lorsque les personnes ne peuvent pas utiliser Signal (ou autre application de votre choix), ni leur ligne téléphonique, ni l'internet ? Il pourrait y avoir un réseau surchargé, un blocage de réseau ou des téléphones vidés de leur batterie. Disposez-vous d'un accès internet de secours

comme un wifi portable par exemple ? Que faire si les données mobiles tombent également en panne ? Avez-vous un plan en mode « hors ligne » ? Est-ce que vous disposerez d’une station de recharge pour les bénévoles et leurs téléphones ?

Ressources supplémentaires

- Guide pratique : utiliser Signal pour iOS https://ssd.eff.org/fr/module/guide-pratique-utiliser-signal-pour-ios
- Guide pratique : utiliser Signal pour Android https://ssd.eff.org/fr/module/guide-pratique-utiliser-signal-pour-android
- Comment vérifier les numéros de sécurité et les mots de sécurité sur Signal (en anglais) https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/



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 :

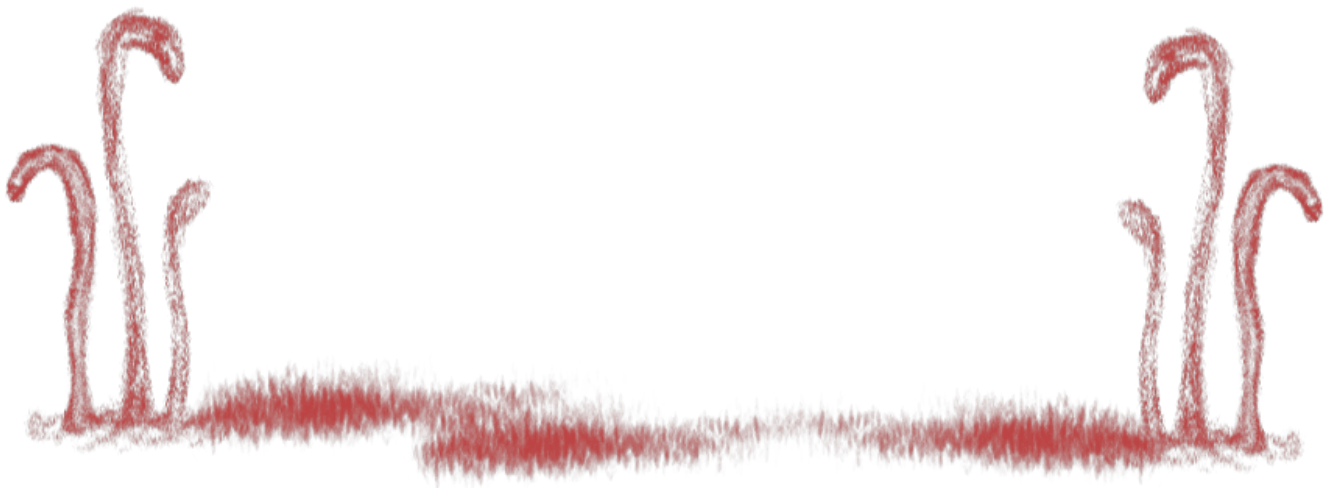
- Dans quel genre de situation avez-vous à réfléchir à votre sécurité physique et à celle de votre téléphone ?
- Que faites-vous déjà pour prendre soin de vous-même dans ces situations ? Pensez au avant, pendant et après.

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

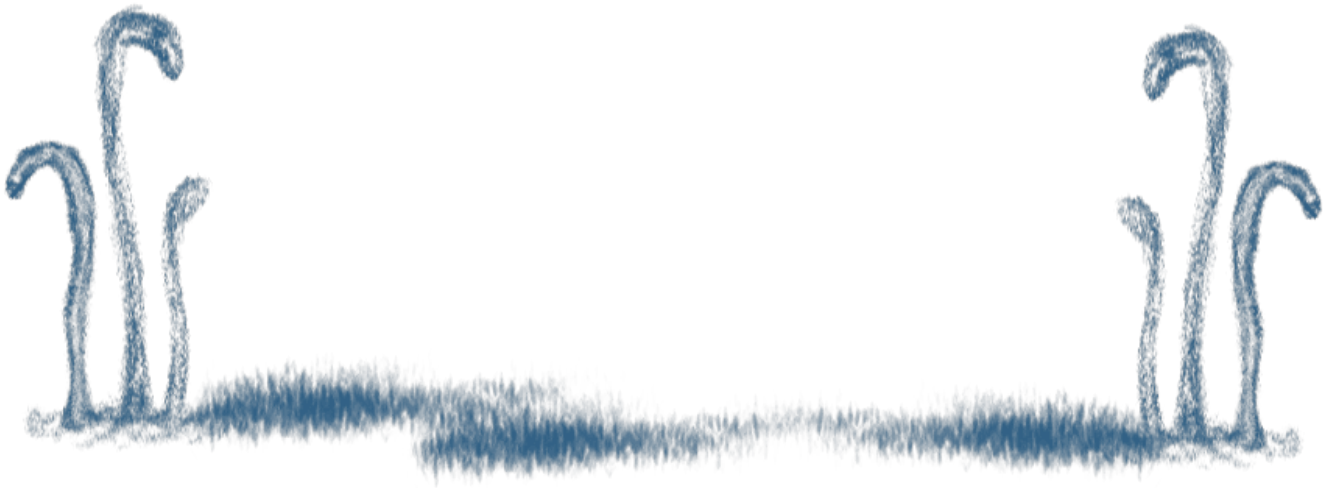
- Effacement à distance
- Application PixelKnot pour chiffrer vos messages (https://guardianproject.info/fr/apps/info.guardianproject.pixelknot/)
- Application Firechat pour les manifestations et les blocages de réseau

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



Choisir nos applications mobiles [activité tactique]

Cette activité comporte une discussion et une présentation qui permettront aux participant·e·s de choisir les applications mobiles qui leur conviennent et qu'iels pourront utiliser après la formation.

activ_tact_FR.png
Image not found or type unknown

Cette activité comporte une discussion et une présentation qui permettront aux participant·e·s de choisir les applications mobiles qui leur conviennent et qu'iels pourront utiliser après la formation.

Cette activité se déroule en 3 étapes :

- Discussion : Qu'est-ce que vous utilisez déjà et pourquoi ?
- Présentation : Les meilleures façons de choisir des applis
- Exercice pratique : Évaluer les applis de messagerie OU Évaluer des applications populaires

Objectifs d'apprentissage

- comprendre la sécurité mobile, en considérant les téléphones mobiles comme nos outils de communications personnelles, privées, publiques et militantes
- 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 ?

À toute personne ayant déjà utilisé un téléphone mobile et qui souhaite mieux savoir comment choisir des applications.

Note sur l'intersectionnalité
Cette activité a été conçue pour évaluer la sécurité des applications mobiles et plus particulièrement des applications de messagerie. D'autres types d'applications pourraient être plus pertinentes pour vos participant·e·s, voici quelques exemples :

- applications de suivi des menstruations ou de fertilité qui collectent des données et qui offrent certaines méthodes de contraception
- applications de rencontres
- applications de messagerie et applications avec suppression immédiate
- applications de sécurité, par exemple celles conçues pour les femmes (ce qu'on peut décider d'y révéler, ce qu'on peut activer ou désactiver, s'il y a un accès à distance, etc.)
- applications de jeu et autre applications interactives
- applications comme tik tok ou OnlyFans

Temps requis

Environ **1 heure.**

Matériel

- du papier pour que les groupes puissent prendre des notes
- un tableau blanc ou de grandes feuilles pour prendre en notes les discussions
- quelques téléphones mobiles avec un accès internet et un accès aux magasins d'applications

Mécanique

Discussion : Qu'est-ce que vous utilisez déjà et pourquoi ? - 10 minutes

En grand groupe, posez les questions suivantes : Quelles sont les 5 applications que vous utilisez le plus ? Vous les utilisez pour faire quoi ? Encouragez tout le monde à participer à la discussion.

- Sur un tableau, prenez en notes les applications mentionnées, demandez combien de personnes les utilisent et écrivez le nombre d'utilisatrices·teurs à côté.
- Écrivez la liste des raisons pour lesquelles iels utilisent ces applis.

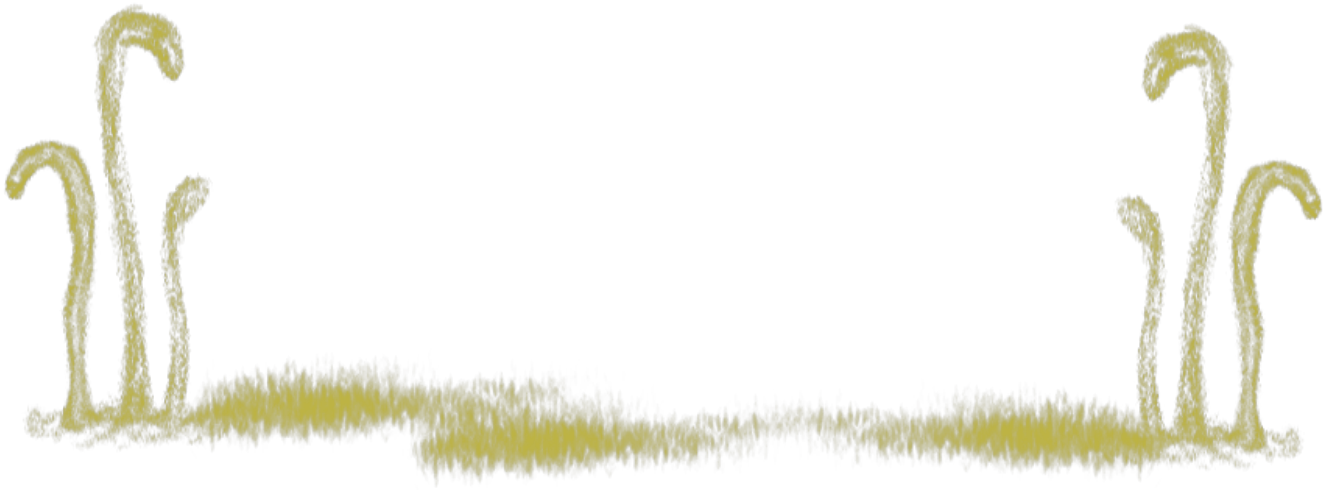
Puis, demandez-leur comment iels les ont choisis.

- Écrivez leurs réponses sur le tableau.

Résumez ensuite leurs réponses et enchaînez avec la présentation.

Présentation : Les meilleures façons de choisir des applis - 5 minutes

- **Faites vos recherches !** Apprenez à connaître les différentes options et apprenez à connaître les applications dignes de confiance. Demandez aux participant·e·s quelles sont leurs méthodes de recherche. Ex. : Lire quelque chose sur internet ou ailleurs, demandez à une amie qui s'y connaît bien, lire les évaluations et les commentaires dans l'App Store ou le Play Store.
- Comment pouvez-vous vous assurer que l'application est sûre ? Qui l'a développée ? Qui la possède ? Quelle est leur politique en matière de vie privée ? Est-ce qu'elle est open source ? Est-ce que l'application est connue pour revendre vos données personnelles à de tierces parties ? Y a-t-il des incidents connus où l'application a été utilisée pour accéder à des appareils personnels ?
- Comprendre les autorisations demandées par vos applications. Par exemple, pourquoi une application de jeu a-t-elle besoin d'accéder à votre caméra et à vos contacts ?
- Qu'est-ce qui vous donne confiance envers cette application ? Pouvez-vous y contrôler les autorisations ? Savez-vous où sont stockées vos informations et celles que vous générez en utilisant l'appli ? Savez-vous où vont ces informations ?
- Est-ce une application « sociale » ? Comment voulez-vous interagir avec les autres sur cette application ? Pouvez-vous contrôler ce qui est visible pour les autres (pseudos, courriel, numéro, contacts, abonné·e·s, « ami·e·s », etc.) ? Pouvez-vous choisir les personnes pour qui vous êtes visible ? Comment les gens peuvent-ils interagir avec vous et vice versa ? Quels sont les paramètres par défaut ? Et qu'est-ce qu'ils révèlent sur vous et vos interactions ? Y a-t-il des problèmes de sécurité avec cet outil ? Est-ce qu'il y a des mécanismes de signalements ? Est-ce que ces mécanismes pourraient être utilisés contre vous ?



Exercice pratique : Évaluer les applications populaires - 15 minutes

Allez dans votre magasin d'applis (App Store, Play Store, etc.) et essayez de trouver une application populaire et utile dans votre contexte. Par exemple, si vous êtes dans un environnement urbain, vous pourriez regarder les applications de taxis ou une application de transport en commun.

Comment choisir ?

D'abord, vérifiez quelles sont les autorisations demandées par l'appli.

Ensuite, vérifiez qui possède, développe et gère cette application.

Il y a beaucoup d'applications qui sont en fait des copies d'applications populaires. Elles sont là pour ressembler à ce que vous cherchez et pour obtenir vos informations de façon malintentionnée . Certaines peuvent se faire passer pour une application de carte de métro ou un jeu et servent en fait à envoyer votre position à quelqu'un d'autre.

Pour prévenir ce genre de situation, vérifiez dans votre App Store qui est la compagnie ou le développeur derrière cette application.

Qu'est-ce que vous savez sur les propriétaires et conceptrices·teurs de l'application ? Faites des recherches pour évaluer si leurs valeurs sont similaires ou différentes des vôtres. Évaluez comment cela peut affecter votre vie privée et votre sécurité si vous utilisez l'application. Si vous avez le choix entre plusieurs applications qui semblent identiques, cherchez en ligne pour obtenir plus d'informations sur l'application et ses développeurs·euses/propriétaires. Vérifiez que vous téléchargez la bonne appli.

Exercice pratique : Évaluer les applications de messagerie - 30 minutes

Formez des petits groupes.

En petits groupes :

- identifiez 2 ou 3 applications de messagerie que vous utilisez
- répondez aux questions-guides suivantes

Questions-guides pour évaluer ces applis :

- Qui utilisent cette appli parmi vous ? Est-elle facile à utiliser ?

- Qui la possède ? Qui gère l'application ?
- Où vos messages sont-ils stockés ?
- Est-ce que les messages sont chiffrés ? Quels sont les autres paramètres de sécurité de cette application ? De quelles façons protégez-vous vos communications quand vous utilisez cette application ?
- Dans quel contexte est-ce une bonne idée de l'utiliser ?
- Dans quel contexte est-ce une mauvaise idée de l'utiliser ?

En grand groupe : Demandez à chaque équipe de présenter une application qu'iels ont évaluée jusqu'à ce qu'elles soient toutes présentées.

Quelques applications de messageries et considérations

SMS

- Tout le monde utilise les SMS.
- Dépendent des opérateurs de téléphonie mobile. Particulièrement risqué s'il y a un historique de collusion entre le gouvernement et ces compagnies, ou si la compagnie est possédée par l'État ou si la compagnie est corrompue.
- Messages stockés par le fournisseur de téléphonie mobile. Les politiques de stockages varient d'une compagnie à l'autre. Les messages que vous envoyez à vos destinataires sont transmis aux tours et antennes de la compagnie.
- Pas de chiffrement.
- Bon moyen de communication pour les sujets sans risque.
- Très souvent, chaque message SMS a un coût.

Appels

- Tout le monde les utilise.
- Les opérateurs et compagnies mobiles en ont le contrôle.
- Stockés chez la compagnie mobile (les métadonnées, c'est certain). Risque d'être écoutés.
- Exemple « Hello, Garcie ! » : Incident connu aux Philippines où un appel entre l'ex-présidente (Arroyo) et le chef de la Commission sur les élections a été intercepté. Dans cet appel, Arroyo lui demandait l'avance électorale qu'elle souhaitait avoir lors des prochaines élections.
- Bon moyen de communications pour les sujets non-risqués.
- Très souvent, chaque appel a un coût.

Facebook Messenger

- N'importe quelle personne qui a un compte Facebook peut l'utiliser.
- C'est une application séparée.
- Le chiffrement est promis mais non vérifié. (Vérifiez cette information, elle pourrait avoir changé.)
- Appartient à Facebook.

- Plutôt que d’utiliser l’application Messenger, utilisez Chat Secure. Vous pouvez utiliser votre compte Facebook pour vous connecter à Chat Secure et discuter avec d’autres utilisateurs·trices Facebook. Pour que le chiffrement fonctionne, les autres personnes doivent aussi utiliser Chat Secure.
- Gratuit, mais nécessite une connexion internet ou des données mobiles payantes.

GoogleTalk

- N’importe qui avec un compte Google.
- Application séparée.
- Promesse de chiffrement, mais non vérifié.
- Appartient à Google.
- Vous pouvez aussi utiliser Chat Secure avec GoogleTalk.

Signal (application recommandée)

- Géré et possédé par des militant·e·s geek indépendant·e·s.
- Chiffrement bout-en-bout.
- Pas de stockage sur le nuage. Les messages sont uniquement stockés sur votre téléphone ou votre ordinateur. Signal ne sauvegarde pas les messages une fois qu’ils sont reçus.
- Appels chiffrés aussi.
- Utilisée pour des communications sensibles ou risquées.

Telegram

- Application de messagerie populaire
- Chiffrement bout-en-bout (avec les discussions secrètes seulement)

WhatsApp

- Un nombre important d’utilisatrices et d’utilisateurs
- Facebook possède WhatsApp. Les développeurs de WhatsApp promettent de préserver la vie privée des utilisateurs·trices dans leur politique. (Leur politique a changé en 2021. À vérifier.)
- WhatsApp sauvegarde seulement les messages non-reçus.
- Chiffrement bout-en-bout, mais si les messages sont sauvegardés avec votre courriel, ils ne sont plus chiffrés.
- Utile pour communiquer avec beaucoup de gens.
- Inquiétant que ce soit possédé par Facebook

Wire

- Promesse de chiffrement bout-en-bout, présentement en cours de vérification (à vérifier)
- Conçu par des anciens développeurs de Skype. (À noter que Skype a déjà construit des backdoors pour le gouvernement chinois)
- Appels vocaux chiffrés

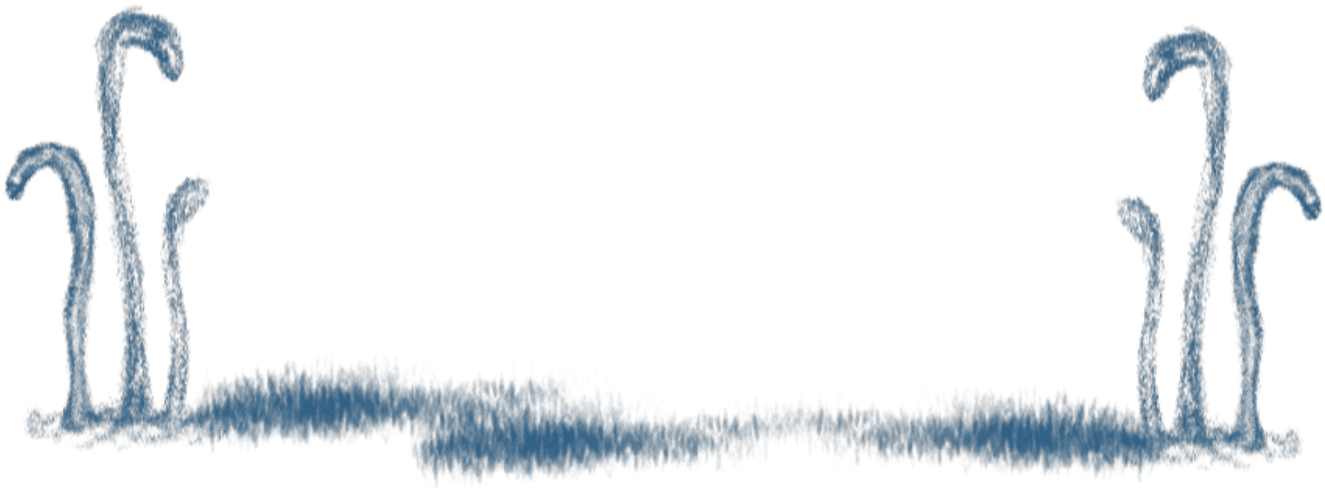
Ressources supplémentaires

- Astuces, outils et guides pratiques pour des communications en ligne plus sécurisées : https://ssd.eff.org/fr
- Qu’est-ce le chiffrement? (MyShadow, en anglais) : https://myshadow.org/alternative-chat-apps#end-to-end-encryption-amp-perfect-forward-secrecy
- WhatsApp : voici les 5 meilleures messageries alternatives : https://www.phonandroid.com/whatsapp-meilleures-messageries-alternatives.html
- WhatsApp ou Signal ? Voici comment choisir son application de messagerie : https://www.phonandroid.com/whatsapp-signal-voici-comment-choisir-application-messagerie.html
- Applications de messagerie alternatives (MyShadow, en anglais) : https://myshadow.org/alternative-chat-apps

> Nous recommandons de faire une recherche sur les derniers problèmes de sécurité des applications que vous prévoyez présenter en atelier. En fonction de ce que vous trouvez, vous voudrez peut-être retirer de votre formation une application présentant des problèmes de sécurité connus et non résolus.

Termes conseillés pour votre recherche :

- Nom de l’application + enjeux de sécurité
- Nom de l’application + politique de confidentialité
- Nom de l’application + vie privée
- Nom de l’application + évaluation de la sécurité



Documenter la violence : Planification et exercice pratique [activité tactique]

Cette activité tactique est destinée aux activistes qui veulent utiliser leurs téléphones mobiles pour documenter des violences. Les participant·e·s vont s’exercer à faire une évaluation des risques et à planifier leur action de documentation avec appareil mobile.

activ_tact_FR.png
image_not_found or type unknown

Cette **activité tactique** est destinée aux activistes qui veulent utiliser leurs téléphones mobiles pour documenter des violences. Les participant·e·s vont s’exercer à faire une évaluation des risques et à planifier leur action de documentation avec appareil mobile. Iels pourront aussi essayer différentes applications et outils sur leurs téléphones et s’exercer à filmer/enregistrer/documenter de façon plus sûre.

> **Conseil care et bien-être :** Cette activité est longue et pourrait prendre la majeure partie de votre journée de formation. Prévoyez des pauses pendant l’activité. Prenez le temps de mentionner et de reconnaître que l’acte de documenter des violences peut être stressant. Encouragez les participant·e·s à partager les trucs qui les aident dans ces situations (ex. : exercices de respiration, exercices physiques ou étirements).

Cette activité se déroule en 2 étapes :

- **Étape 1 : Évaluation et planification**
  Les participant·e·s devront d’abord planifier leur action : en évaluant les enjeux de sécurité et en prenant en compte le bien-être des personnes concernées. En fonction de cette évaluation, iels établiront des plans de sécurité et décideront des meilleures façons d’utiliser leurs téléphones.
- **Étape 2 : Préparation du téléphone et exercice pratique**
  Ensuite, les participant·e·s pourront s’exercer à utiliser leurs téléphones pour documenter des violences. Iels développeront des stratégies et tactiques en ce sens.

Pour accompagner cette activité, nous recommandons également les activités Débat : Documenter la violence et On a saisi mon téléphone ! : Sauvegarde, verrouillage et suppression.

Objectif d’apprentissage

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 ?

Aux groupes qui utilisent ou qui souhaitent utiliser les téléphones mobiles pour documenter des violences.

Temps requis

Au moins **1h45 min**. *(Cette activité peut être longue, prévoyez des pauses.)*

Matériel

- Des études de cas imprimées ou des liens vers des études de cas

Mécanique

Introduction - 5 minutes

Commencez par présenter quelques exemples de mouvements sociaux qui utilisent ou qui ont utilisé les téléphones pour documenter des violences. Demandez aussi au groupe de donner des exemples : sur leurs propres expériences de documentation ou de diffusion de ces images. Voici quelques exemples possibles : documenter les violences de l’État, transférer des vidéos d’actes violents, les risques qui viennent avec le fait de posséder ce genre d’images, etc.

Étape 1 : Évaluation et planification - 30 minutes

Invitez les participant·e·s à former des petits groupes en fonction de leurs expériences communes de documentation de violences.

Conseil *care* et bien-être : Encouragez vos participant·e·s à évaluer et planifier en fonction de leurs propres besoins et limites personnelles. Documenter des actes de violence peut être très bouleversant et angoissant. Encouragez-les à partager avec le groupe leurs trucs pour préserver leur bien-être et prendre soin d'elleux-mêmes. Iels peuvent aussi mentionner leurs façons de gérer collectivement (avec leurs camarades activistes) les impacts de ce genre d'action.

Voir aussi : On a saisi mon téléphone ! : Sauvegarde, verrouillage et suppression

Discussion : Les objectifs de votre action

- Qu'est-ce que vous voulez documenter ? Et pourquoi ?
- Quel est le contexte ?
- Dans quel but souhaitez-vous faire cette action ? Si l'objectif est d'accumuler des preuves, vérifier les exigences judiciaires en matière de preuves. Pour plus d'informations à ce sujet, consultez la section « La preuve par vidéo » de WITNESS :

  https://fr.witness.org/ressources/la-preuve-par-video/

Discussion : Évaluation des risques et bien-être des personnes concernées

Discutez des risques connus ou potentiels de votre action pour toutes les personnes concernées : c'est-à-dire les personnes qui documenteront et les personnes qui seront filmées ou « documentées ».

- À quels enjeux de sécurité ferez-vous face pendant cette action ? Risquez-vous de tomber sur la police ou sur des adversaires ?
- Qu'est-ce qui pourrait changer et vous mettre en danger au cours de votre action ? Comment pouvez-vous vous y préparer ? Comment réagirez-vous ? Discutez de scénarios probables. Exemple de scénario : que faire lorsque la police ou des adversaires deviennent plus violents ? Exemples de réactions anticipées : continuer de documenter/filmer, augmenter le rythme des messages au sein de votre équipe (aviser de votre état de sûreté), arrêter de documenter/filmer/etc.
- Qui participera à votre action et aux différentes tâches (filmer, soutien, communications internes, réseaux sociaux, etc.) ? De quel soutien ces personnes ont-elles besoin ?
- Y a-t-il des enjeux de sécurité qui préoccupent des membres de votre équipe ? Est-ce que des personnes se sentent moins en sécurité de participer à l'action à cause de son contexte (ex. : à cause du type de violence en jeu) ? Y a-t-il des tâches que ces personnes sont plus à l'aise de faire ?
- Quelles sont vos stratégies pour vous garder en sécurité (vous, votre équipe et vos allié·e·s) pendant l'action ?
- Comment le consentement entre-t-il en jeu dans votre action de documentation ? Est-ce que vous demanderez le consentement des personnes que vous filmez ? Comment ces personnes pourront-elles donner leur consentement à être filmées ou enregistrées ? Est-

ce que vous demanderez aussi leur consentement en lien avec la diffusion des images plus tard ?
- Y a-t-il des questions de sécurité liées à la possession de ces images ? Y a-t-il des enjeux de sécurité pour les personnes qui apparaissent dans les images ? Que ferez-vous avec ces images pour les protéger ? Où et comment seront-elles stockées ? Qui y aura accès ? Est-ce qu'elles seront chiffrées ? Quand seront-elles supprimées ?
- Quels seront les impacts sur vous si vous prenez part à cette action de documentation ? De quoi aurez-vous besoin pour être bien et solide pendant cette action ? Quelles sont les ressources que les autres peuvent vous fournir pour vous soutenir ? Comment allez-vous vous soutenir en tant qu'équipe ? Quels sont les besoins (soutien, ressources) de vos camarades ? Comment votre équipe pourra-t-elle répondre à ces besoins ?

Connaissez vos droits

- Dans votre région, quels sont vos droits liés au fait de documenter de violences ?
- Quels sont vos droits selon le contexte de votre action ? À savoir, quels sont vos droits par rapport au fait de filmer la police ? Est-ce légal ? Est-ce que les rassemblements sont considérés illégaux ?
- Est-ce que la police a le droit de fouiller vos appareils ?
- Est-ce que la police est connue pour fouiller les appareils et pour forcer les gens à supprimer des images ?

Préparez votre appareil mobile

- Est-ce que vous utilisez votre téléphone personnel ?
- Quels fichiers allez-vous supprimer de votre téléphone ? Pourquoi ?
- Quelles applications allez-vous installer ou désinstaller ? Pourquoi ?
- Localisation : Est-il plus sûr d'activer ou de désactiver votre localisation ? Est-ce que vous voulez que des collègues ou personnes de confiance puissent suivre votre localisation ?
- Effacement à distance : Voulez-vous activer l'option d'effacement ou de suppression à distance ? Au cas où vous perdriez l'accès à votre téléphone.

Discussion : Utiliser son téléphone personnel, oui ou non ?

Complément d'information

Utilisez les informations de l'activité La téléphonie mobile : Comment ça marche ? pour expliquer : comment les téléphones mobiles peuvent permettre de nous identifier ; la surveillance et l'identification en temps réel ; comment les métadonnées générées par notre téléphone et les données EXIF (des photos, vidéos) peuvent servir à nous identifier.

Après l'action

- Prévoyez de vous réunir pour faire un retour sur l'événement. Comment cela s'est-il passé ? Des choses inattendues se sont-elles produites ? Comment avez-vous réagi ? Y a-

t-il encore des choses pour lesquelles vous devez répondre ou réagir ? Comment l'équipe se sent-elle ? Qui veut participer aux prochaines tâches ?
- Diffusion et partage : Revérifiez vos ententes liées au consentement et à la diffusion (publication, partage) des images. Assurez-vous de partager ces ententes avec toute personne qui aura accès aux images.

Discussion

Que voulez-vous faire d'autre après cette action de documentation ?

Étape 2 : Préparation du téléphone et exercice pratique - 1 heure

Selon le temps que vous avez, vous pouvez faire cette étape en grand groupe ou en petites équipes. En petites équipes, les gens peuvent se joindre au groupe qui convient le plus à leurs besoins.

Quelques trucs

Comment utiliser la photo, la vidéo ou l'audio pour documenter des violences :

- Trouvez les outils intégrés à votre téléphone : caméra, enregistrement audio, etc.
- Exercez-vous à utiliser ces outils. Suivez les conseils du guide « Filmer avec un téléphone portable » : https://fr.witness.org/portfolio_page/filmer-avec-un-telephone-portable/
- **Photos et vidéos : Choisissez bien vos cadrages**
  - **Détails et perspective :** approchez-vous physiquement pour capturer plus de détails et reculez-vous pour obtenir une perspective plus large d'un l'événement

    - **Des images stables :** cadrez bien votre sujet et tenez fermement votre appareil pendant au moins 10 secondes, utilisez vos deux mains et collez vos coudes sur votre corps pour être plus stable. Évitez d'utiliser le zoom. Évitez d'avoir des images qui bougent.
    - Tenez votre téléphone **horizontalement** pour obtenir un plan plus large.
    - Approchez-vous pour une **meilleure qualité sonore :** les sons ambiants peuvent enterrer vos entrevues.
    - **Éclairage :** filmez dans un lieu bien éclairé et évitez de filmer à contre-jour.

- Si vous avez beaucoup de temps, vous pouvez travailler en équipe pour créer une vidéo.
- Si vous décidez de publier votre vidéo sur Youtube, pensez à utiliser l'option des sous-titres : https://support.google.com/youtube/answer/2734796?hl=fr
- Contexte et message : Préparez bien votre message. Où allez-vous publier vos images ? Quel texte accompagnera vos images ? Comment ferez-vous le lien avec vos objectifs plus généraux ?

Enregistrer des appels

> **Remarque :** Cette option s'est montrée utile pour les travailleuses·eurs du sexe subissant des menaces de la part des autorités.

Avec une application

Vous pouvez installer une application qui permet d'enregistrer des appels. Vous aurez besoin d'une connexion internet (ou de données mobiles) pour télécharger l'application et pour l'utiliser pendant vos appels. Ceci nécessitera une certaine planification.

- Choisissez une application qui répond à vos besoins et installez-la.
    - Google Voice vous permet d'enregistrer les appels entrants seulement.
    - Vérifiez si vous avez une application déjà intégrée à votre téléphone.
- Testez l'application avec une autre personne.
- Exercez-vous à trouver le fichier sur votre téléphone et à l'enregistrer ailleurs : dans un lieu sûr où vous pourrez y accéder au besoin.

Avec un enregistreur vocal

Si vous décidez de ne pas utiliser une application d'enregistrement d'appels ou si vous n'arrivez pas à le faire, vous pouvez vous exercer à utiliser un enregistreur vocal. En mettant votre téléphone en mode « haut-parleur », vous pourrez enregistrer l'appel avec votre magnétophone ou avec un autre téléphone mobile. Certains téléphones ont une option intégrée d'enregistrement vocal qui vous permettra de le faire.

- Choisissez l'application ou l'outil qui répond à vos besoins et installez-le.
- Faites un test avec une autre personne. Pour une meilleure qualité sonore, enregistrer dans un endroit calme sans grands bruits de fond.

- Exercez-vous à trouver le fichier sur votre téléphone et à l'enregistrer ailleurs : dans un lieu sûr où vous pourrez y accéder au besoin.

Captures d'écran

Vous pouvez prendre des captures d'écran sur votre téléphone pour documenter du harcèlement et des violences.

- Choisissez une application pour y tester des captures d'écran (ex. : sur Facebook, ou une application de messagerie) :
  - *Sur Android :* Sur les téléphones Android (avec la version Ice Cream Sandwich), vous pouvez appuyer simultanément sur le bouton d'alimentation et sur celui pour réduire le volume. Maintenez pendant une seconde et votre téléphone fera une capture d'écran qui sera enregistrée dans votre galerie.
  - *iPhone X, XS, XR* : Appuyez simultanément sur le bouton latéral à droite et sur le bouton pour hausser le volume. La capture d'écran sera enregistrée dans vos albums (dans un album nommé « Captures d'écran »).
  - *iPhone 8 et autre modèle plus récent* : Appuyez simultanément sur le bouton d'alimentation à droite et sur le bouton principal. La capture d'écran sera enregistrée dans vos Photos, dans un album nommé « Capture d'écrans ».
- Exercez-vous à trouver le fichier sur votre téléphone et à l'enregistrer ailleurs : dans un lieu sûr où vous pourrez y accéder au besoin.

> **Attention !** Vous ne pourrez pas faire des captures d'écran de n'importe quelle application. Certaines applications, comme Signal, ont des paramètres de sécurité qui bloquent les captures d'écran dans certaines conversations.

Documenter des événements pour vos rapports internes

Lorsqu'un incident se produit, qu'il soit bref, long, isolé ou répété, il est important de documenter et noter les informations sur l'événement. Bien que plusieurs des tactiques présentées ici concernent la documentation dans un but de diffusion publique, il est aussi utile de le faire dans un but interne. Prenez note des informations suivantes : Où s'est produit l'incident ? Quand cela s'est-il passé ? Qui est impliqué·e dans l'événement ? Que s'est-il passé ? En conservant ces informations, cela pourrait être utile pour reconstituer les événements, évaluer et planifier des ripostes, si nécessaire.

Diffusion en direct

Cette section est inspirée du guide Diffusion de manifestations en direct (en anglais) écrit par WITNESS pour les militant·e·s aux États-Unis.

Vous souhaitez diffuser en direct un événement comme une manifestation ou un rassemblement. Avant tout, prenez le temps de faire les activités d'évaluation et de préparation présentées à

l’Étape 1. La diffusion est une bonne façon de montrer des événements en temps réel et d’inciter les gens qui regardent à soutenir la cause en jeu. Il faut prendre en compte les risques élevés qui viennent avec cette diffusion : comme la présence policière sur place ou la surveillance policière qui ciblent des activistes (pendant ou après la diffusion en direct).

- **Lieux :** Montrez volontairement l’emplacement des événements. Filmez les noms des rues, les édifices et tout autre point de repère permettant d’identifier les lieux. D’ailleurs, prenez en considération comment le fait de révéler votre position en temps réel est lié à votre propre sécurité et à celle des personnes que vous filmez.
- **Identification des participant·e·s :** Serez-vous en mesure de demander le consentement des personnes que vous filmez ? Comment voulez-vous protéger leur identité ? Comment pouvez-vous le faire ? Songez à ne pas filmer les visages.
- **Identification des tactiques :** Ceci fonctionne dans les deux sens. Vous pourriez involontairement filmer les tactiques des militant·e·s d’une manière qui pourrait leur nuire. D’un autre côté, vous serez peut-être en mesure de filmer les tactiques policières et ainsi mieux appréhender leurs formations et actions probables à l’avenir.
- **Votre public cible :** Quels sont les objectifs de votre diffusion en direct ? Voulez-vous le faire pour un petit groupe de confiance qui pourrait vous soutenir en retravaillant vos images ?
- **Travaillez en équipe :** En travaillant en équipe, vous pourrez faire plusieurs tâches de façon plus efficace et partagée. Certaines personnes peuvent vous soutenir en interagissant dans les commentaires de la diffusion en direct, d’autres peuvent se charger de partager la diffusion sur différents canaux.
- **Proposez une action :** Invitez vos téléspectateurs et téléspectatrices à agir.
- **Votre appareil :** Souhaitez-vous utiliser votre téléphone personnel ? Quel que soit l’appareil que vous utilisez, chiffrez-le et protégez-le avec un mot de passe. N’utilisez pas l’option de l’empreinte digitale.

Retour en grand groupe - 10 minutes

Faites un retour en grand groupe pour discuter du pourquoi nous documentons des violences. Prenez le temps de reconnaître que ce travail est angoissant.

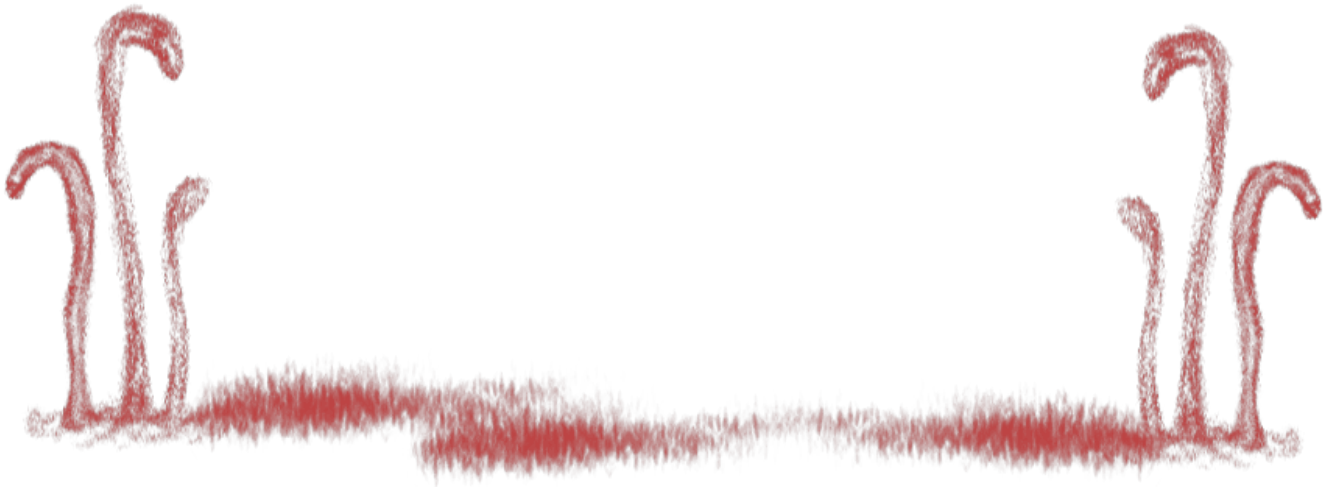
Invitez les participant·e·s à présenter ce qu’iels ont créé dans leurs petits groupes.

Invitez-les à présenter ce qu’iels ont appris, les nouveaux outils qu’iels ont explorés et les trucs qu’iels ont développés.

Ressources supplémentaires

- De l’usage des caméras en manifestation : https://lundi.am/De-l-usage-des-cameras-en-manifestation

- Le réseau Video For Change : https://video4change.org/
- « La preuve par vidéo » (WITNESS) : https://fr.witness.org/ressources/la-preuve-par-video/
- Guide « Faire des vidéos en équipe : Manifestations et rassemblements » (WITNESS) : https://fr.witness.org/portfolio_page/faire-des-videos-par-equipe/
- Guide « Filmer avec un téléphone portable » (WITNESS) : https://fr.witness.org/portfolio_page/filmer-avec-un-telephone-portable/
- « Mener des entrevues sûres, efficaces et éthiques de survivant·e·s de violence à caractère sexuel et sexiste » (WITNESS) : Guide vidéo (sous-titré en français) et document PDF.
- « Diffusion de manifestations en direct - États-Unis » (WITNESS) : https://fr.witness.org/ressources/la-preuve-par-video/
- Métadonnées des vidéos (vidéo sous-titrée en français) : https://library.witness.org/product/video-metadata/
- UWAZI, est une plateforme gratuite et à code ouvert qui permet d'organiser, d'analyser et de publier vos documents. L'outil a été créé pour soutenir le travail des défenseur·e·s des droits humains. https://www.uwazi.io/



Applis de rencontres, vie privée et sécurité [activité tactique]

activ_tact_FR.png
Image not found or type unknown

Dans cette **activité tactique**, les participant·e·s pourront s’échanger des trucs et conseils en lien avec les rencontres en ligne et les applications de rencontres. Les participant·e·s travailleront en petits groupes et en binômes pour mettre à jour leurs profils sur des sites de rencontres. Les participant·e·s pourront nommer leurs différents besoins et leurs préférences entourant les applis de rencontres, la vie privée et la sécurité. Iels pourront s’échanger des stratégies pour mieux protéger leur vie privée sur les applis de rencontres. Iels pourront aussi mettre en pratique ces stratégies pendant l’atelier.

> **Remarque sur l’intersectionnalité :** Ouvrez les discussions afin que les participant·e·s puissent s’exprimer sur leur expérience en lien avec leur genre et leur sexualité. Laissez-les discuter des relations entre leur genre/sexualité et leur expérience des rencontres en ligne. Comment cela influence-t-il leurs préoccupations en termes de vie privée et de sécurité ? Est-ce que leur genre et sexualité sont représentés dans les applications populaires ?

Cette activité se déroule en 2 étapes :

- Rencontres en ligne : Échanger des trucs et conseils de sécurité
- Exercice pratique : Mettre à jour nos profils

Objectifs d’apprentissage

- comprendre en quoi les communications mobiles et leur accès sont genrés et intimes
- comprendre la sécurité mobile, en considérant les téléphones mobiles comme nos outils de communications personnelles, privées, publiques et militantes
- 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 ?

Aux personnes qui utilisent des applications de rencontres et qui veulent les utiliser de façon plus sûre.

Temps requis

Environ **2h-2h30.**

> **Conseil pour l’animation :** Nous recommandons de faire quelques pauses pendant cette activité.

Matériel

- Accès internet
- Des téléphones mobiles pour mettre à jour des profils de rencontre
- Tableau blanc ou tableau à feuilles mobiles

Mécanique

Rencontres en ligne : Échanger des trucs et conseils de sécurité

Activité brise-glace - 5 minutes

- Qui utilise des applications de rencontres ? Lesquelles utilisez-vous ? Comment et pourquoi les avez-vous choisies ?
- De quelles façons protégez-vous votre sécurité et vie privée sur ces applis ?

Des rencontres plus sûres - 30 minutes

Avant de vous lancer dans les applications et les exercices pratiques, invitez les participant·e·s à échanger leurs trucs pour des rencontres en ligne plus sûres.

Questions :

- Selon vous, qu’est-ce qu’un « comportement sûr » lorsqu’on utilise des applis de rencontres ?
- Qu’est-ce que vous prenez en considération lorsque vous décidez de rencontrer l’autre en personne ?
- Quelles sont vos stratégies pour « savoir » quand vous pouvez rencontrer une nouvelle personne en personne ?
- Avez-vous un plan B au cas où les choses tournent mal ? Par mesure de sécurité, est-ce que vous vous êtes entendu·e avec un·e ami·e de lui écrire à une certaine heure ? Est-ce que vous dites à une personne de confiance où vous allez et qui vous rencontrez ?

Écrivez leurs réponses sur un tableau pour que ce soit visible pour tout le monde.

Vous pouvez ensuite leur présenter les conseils suivants. Invitez les participant·e·s à en ajouter des nouveaux :

Conseils de sécurité (applis de rencontres)

- Assurez-vous que votre photo ne donne pas plus d’informations sur vous (comme votre localisation, votre quartier, votre école, etc.)
- Utilisez une adresse courriel sécurisée et alternative pour ce compte
- Choisissez un pseudo qui ne ressemble pas à vos autres comptes de réseaux sociaux
- Utilisez une photo différente de vos autres comptes de réseaux sociaux
- Ne mettez pas d’informations personnelles
- Faites attention et réfléchissez bien à ce que vous écrivez dans votre profil
- Rencontre en personne : Quand vous rencontrez une personne pour la première fois, faites-le dans un endroit public. Si possible, avisez un proche du moment et du lieu de rencontre.
- Choisissez un mot de passe pour les applications quand c’est possible
- Chiffrez et protégez votre appareil avec un mot de passe

Complément d’information : Nouveaux modèles d’applis

Y a-t-il des caractéristiques que vous appréciez particulièrement dans les applications de rencontres existantes et que vous pourriez rechercher dans les nouvelles applications ?

Quelles sont les possibilités et les fonctionnalités offertes par les nouvelles applications (par exemple, signaler d'une manière ou d'une autre les utilisateurs ayant une mauvaise réputation, documenter les escrocs, partager des conseils en matière de rencontres) ?

Comment interagissez-vous déjà avec vos amis de confiance et les membres de votre communauté de rencontre en ligne ?

Exercice pratique : Mettre à jour nos profils - 1h-1h30

Commencez par vous « doxxer » légèrement, c'est-à-dire regarder les informations liées à votre nom dans votre appli de rencontres. Puis, à partir de cette information, cherchez-vous vous-même sur d'autres plateformes (dans un moteur de recherche, sur Facebook, sur Instagram, etc.). Essayez de chercher votre pseudo ou d'autres informations de votre profil de rencontre. Réfléchissez aux informations personnelles qui sont disponibles lorsqu'on fait cette recherche à partir de votre profil. Qu'est-ce que vous voulez garder privé ? Y a-t-il des choses que vous ne voulez pas que les utilisateurs·trices de l'application de rencontres sachent sur vous ?

À partir de ces constats, ré-écrivez votre profil.

En équipes de deux, consultez les **conseils de sécurité** et mettez à jour vos profils. Entraidez-vous dans cet exercice à atteindre vos propres buts en matière de sécurité. Aidez votre partenaire à trouver les informations de leur profil pouvant les identifier, suggérez ensemble des façons de changer vos profils pour les rendre moins identifiables.

Mettez à jour vos photos

Vérifiez si vos images ne correspondent plus aux mesures de sécurité que vous voulez adopter. Remplacez-les, si vous voulez et si cela vous semble nécessaire. Pensez à effacer les métadonnées et dissimuler les informations permettant d'identifier d'autres personnes dans vos photos.

Mettez à jour votre texte

Vérifiez si votre texte révèle plus d'informations personnelles que vous ne le voulez. Si vous voulez, travaillez avec un partenaire !

Créez une adresse courriel sécurisée et alternative

Retour en grand groupe - 10 minutes

Comment cela s'est-il passé pour vous ? Qu'est-ce qui vous a surpris ? Qu'est-ce qui était difficile à faire ? Qu'est-ce que vous ferez de plus suite à cet atelier ?

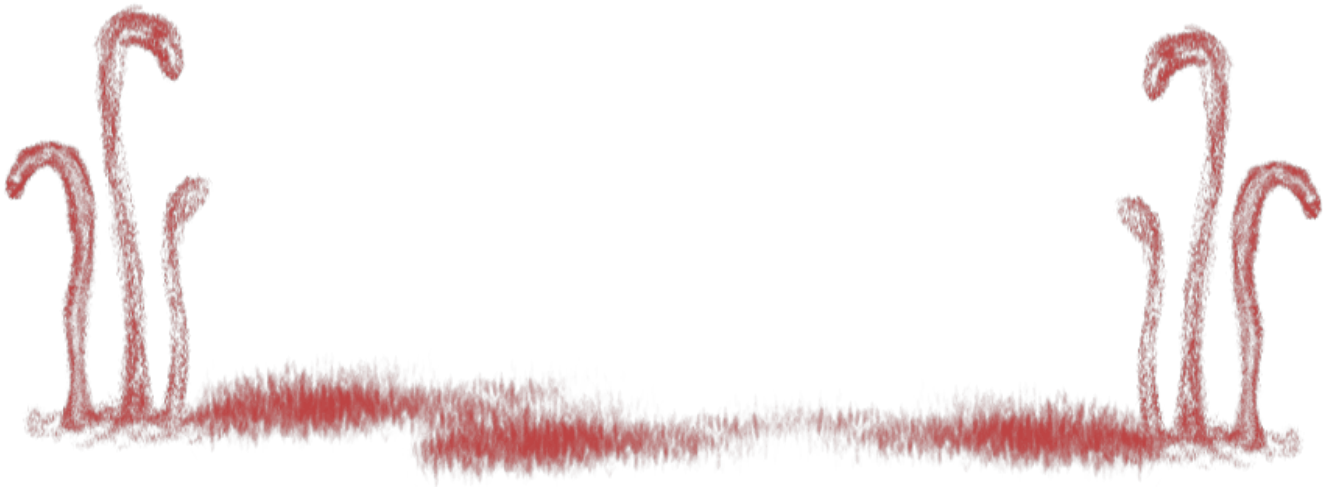
> **Conseil pour l'animation :** Si vos participant·e·s sont intéressé·e·s par les sextos, consultez l'activité Sextos, plaisir et sécurité.

Ressources supplémentaires

Auto-Doxing (en anglais) : https://gendersec.tacticaltech.org/wiki/index.php/Step_1#Self-Doxing

Guides de sécurité (en anglais) et applis de rencontres :

- 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/



Sextos, plaisir et sécurité [activité tactique]

activ_tact_FR.png image not found or type unknown

Dans cette **activité tactique**, les participant·e·s sont invité·e·s à échanger et découvrir des stratégies pour envoyer des sextos de façon plus sûre.

Objectifs d’apprentissage

- comprendre en quoi les communications mobiles et leur accès sont genrés et intimes
- comprendre la sécurité mobile, en considérant les téléphones mobiles comme nos outils de communications personnelles, privées, publiques et militantes
- 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 ?

Aux personnes qui sextent ou qui aimeraient sexter et qui souhaitent discuter de stratégies pour des sextos plus sûrs.

Temps requis

Environ **2 heures.**

Matériel

- Téléphones mobiles
- Accès internet ou données mobiles
- Cartons ou grandes feuilles de papier

Mécanique

Discussions en binômes - 10 minutes

- Est-ce que vous avez déjà sexté ? À quand remonte la première fois que vous avez échangé des sextos ? Quels moyens aviez-vous utilisés ? Ex. : Téléphone fixe, lettres, cartes postales, messagerie instantanée en ligne.
- Comment utilisez-vous votre téléphone pour sexter ? Applications, textos, messages audios, vidéos, etc. Qu'est-ce que vous aimez ? Selon vous, quels sont les avantages et inconvénients de ces options ?
- Quels sont les enjeux de sécurité et de vie privée que vous prenez en compte lorsque vous faites des sextos ? Que faites-vous pour assurer votre sécurité et protéger votre vie privée ?

Retour en grand groupe – échange de stratégies - 35 minutes

Invitez les participant·e·s à échanger sur ce qui est amusant et agréable avec les sextos.

> **Remarque sur l'intersectionnalité :** Est-ce que les sextos sont stigmatisés dans le contexte des participant·e·s ? Est-ce que ceci est influencé par l'identité de genre, la sexualité, la race, la classe ou l'âge ? De quelles manières les gens font-ils face à la désapprobation sociale des sextos ?

Quelques questions pour la discussion:

- Textos, photos, audios, vidéos, etc. : qu'est-ce que vous préférez utiliser ? Quelles sont vos applications préférées ? Qu'est-ce que vous aimez le plus de tout ça ? Qu'est-ce que vous aimeriez pouvoir faire de plus avec ces échanges ou ces applications ?
- Qu'est-ce qui vous apporte le plus de plaisir dans vos sextos ? Et pourquoi ?

Échange de stratégies

Préparez de grands cartons ou des feuilles et écrivez dessus les titres suivants :

- Ententes de sextos
- Nos photos intimes et nos données
- Applications et sécurité
- Sujet libre

Animez une discussion pour chaque sujet. Utilisez les questions-guides plus bas. Écrivez les stratégies des participant·e·s sur le carton.

Ententes de sextos

- Établissez des ententes avec vos partenaires de sextos. Quelles sont vos ententes concernant la sauvegarde des échanges ? Et concernant le partage en ligne ou en personne de ces sextos ?
- Avez-vous déjà négocié des ententes de sextos avec vos partenaires ? Comment avez-vous fait cela ?
- Des ruptures, ça arrive. Est-ce que vous prévoyez une entente en cas de rupture ? Comment négociez-vous avec vos partenaires quand une rupture survient ? Est-ce que vous pouvez conserver leurs sextos et vice versa ?

Nos photos intimes et nos données

Les informations qui sont attachées à nos photos et ce qu'elles racontent :

- Demandez-vous si vous voulez envoyer des photos intimes où l'on peut voir votre visage
- Essayez de cacher les éléments corporels permettant de vous identifier (ex. : tatouages, marques de naissance, etc.)
- Utilisez des outils pour effacer les données EXIF de vos photos (métadonnées, localisation, appareil, date, etc.)
- Utilisez des applications pour flouter votre visage, vos tatouages, etc. (Ex. : Pixlr)

Applications et sécurité

- Choisissez une application qui offre des options de sécurité et de vie privée comme le chiffrement, la suppression de messages, le blocage de captures d'écran, etc.
- Utilisez une application de messagerie sécurisée qui vous donne le contrôle sur vos images et vos messages (que vous pouvez supprimer si vous le voulez)
- **Remarque sur le jargon : « Auto-destruction »** – Certaines applications comme Snapchat promettent d'offrir l'option d'auto-destruction. Toutefois, très souvent, ces messages/images ne sont pas entièrement détruits et les gens peuvent encore les voir et les partager plus tard.
- Définissez un mot de passe et chiffrez votre téléphone
- Définissez un mot de passe sur vos applications
- Songez à utiliser une adresse courriel sécurisée et un numéro de téléphone alternatif pour la création d'un compte sur une application
- Sachez comme supprimer et sauvegarder
- Vérifiez si l'application est synchronisée (avec le nuage par exemple). Vérifiez si vous souhaitez garder cette synchronisation activée.

Exercices pratiques : Applications plus sûres et modifier nos photos

Discussion : Comment choisir nos applis de sextos

Vos participant·e·s utilisent quelles applications pour leurs sextos ? Et pourquoi celles-ci ? Quand vous choisissez une application, quelles sont vos préoccupations en matière de sécurité ? Quelles sont les options de sécurité que vous aimez dans votre application ? Qu'est-ce qui vous préoccupe ?

Utilisez des applications :

- chiffrées
- protégées par mot de passe
- qui empêchent la sauvegarde ou les captures d'écran
- qui permettent de supprimer des messages

À propos des SMS et textos multimédias : ces options de sécurité ne sont pas incluses. Pour plus d'informations sur les SMS et la surveillance, consultez l'activité La téléphonie mobile : Comment ça marche ?.

Exercices pratiques

Ces exercices donnent l'opportunité aux participant·e·s d'essayer des stratégies de sécurité recommandée par les formatrices du FTX. Sélectionnez les exercices qui sont les plus pertinents dans votre contexte. Voici d'autres idées :

- Chiffrer et protéger nos appareils avec un mot de passe
- Effacer les informations nous identifiant sur nos photos et nos téléphones
- Créer une adresse courriel sécurisée pour nos comptes de sextos ainsi qu'un numéro de téléphone alternatif

Faites une liste des étapes pour ces exercices. Invitez les participant·e·s à s'exercer en petits groupes. Invitez-les à s'entraider et à chercher des conseils et réponses sur internet.

Exercice pratique avec vos photos

- Prenez des photos en évitant de montrer votre visage
- Essayez de cacher les éléments corporels permettant de vous identifier (ex. : tatouages, marques de naissance, etc.)
- Utilisez des outils pour effacer les données EXIF de vos photos (métadonnées, localisation, appareil, date, etc.)
- Utilisez des applications pour flouter votre visage, vos tatouages, etc. (Ex. : Pixlr)

Exercice pratique avec votre appareil et vos applis

- Choisissez et installez une application sécurisée
- Définissez un mot de passe pour vos applications
- Sachez comment supprimer et sauvegarder des échanges
- Sachez comment supprimer des images de votre téléphone

Retour en grand groupe - 10 minutes

Comment se sont passés les exercices pratiques ?

- Qu'est-ce que vous avez fait ?
- Invitez les participant·e·s à présenter leurs exemples de photos s'iels le veulent.
- Qu'est-ce qui était plus difficile ? Qu'est-ce qui était facile à faire ? Qu'est-ce qui vous a surpris ?
- Quand vous aviez des questions, où avez-vous cherché l'information ?

Ressources supplémentaires

- 6 outils pour éditer ou supprimer les métadonnées EXIF de vos photos
  https://www.codeur.com/blog/outils-metadonnees-exif/

> **Conseils pour l'animation:** *Comme la suppression des images des applications et des appareils peut être un peu compliquée, voici quelques instructions spécifiques pour aider les participant·e·s à savoir comment supprimer des images de leur appareil (dernière mise à jour en mai 2019) :* Pour savoir comment supprimer des images de votre appareil, il faut comprendre comment le faire dans la mémoire de votre application et connaître l'endroit où vos images sont stockées dans votre téléphone.

Sur les appareils iOS, l'opération est plus opaque, car vous n'avez pas accès aux fichiers en dehors des applications où les fichiers sont générés.

Cela dépend également de comment vous prenez vos photos : Est-ce que vous les prenez directement dans l'application ? Ou est-ce que vous prenez les photos à partir de votre application caméra de votre téléphone ?

Si vous utilisez Telegram, cliquez sur l'en-tête d'une conversation, cliquez sur « Afficher tous les médias », vous pourrez y supprimer des images. Ces images seront supprimées de l'application Telegram. Si vous les avez enregistrées sur votre téléphone, vous devrez les trouver dans votre Galerie pour les supprimer définitivement. Dans Telegram, vous pouvez explorer les médias partagés avec un·e utilisateur·trice ou un groupe.

Pour Signal, cliquez sur l’en-tête d’une conversation, cliquez sur « Tous les médias », vous pourrez y supprimer des images. Ces images seront supprimées de l’application Signal. Si vous les avez enregistrées sur votre téléphone, vous devrez les trouver dans votre Galerie pour les supprimer définitivement. Ceci s’applique également aux personnes à qui vous envoyez des sextos.

Si vous utilisez un téléphone Android, utilisez un gestionnaire de fichiers pour trouver vos images. **Pour Telegram :** Allez dans « Stockage interne », chercher le dossier « Telegram » et supprimez les fichiers désirés.

Pour Signal, vous pouvez enregistrer des fichiers reçus sur le stockage de votre appareil. Vous pouvez choisir à quel endroit vous l’enregistrer dans votre téléphone. Pour les retrouver, allez dans « Stockage interne », puis « Images ». Par défaut, les images sauvegardées à partir de Signal sont enregistrées là.