Image not found or type unknown

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.

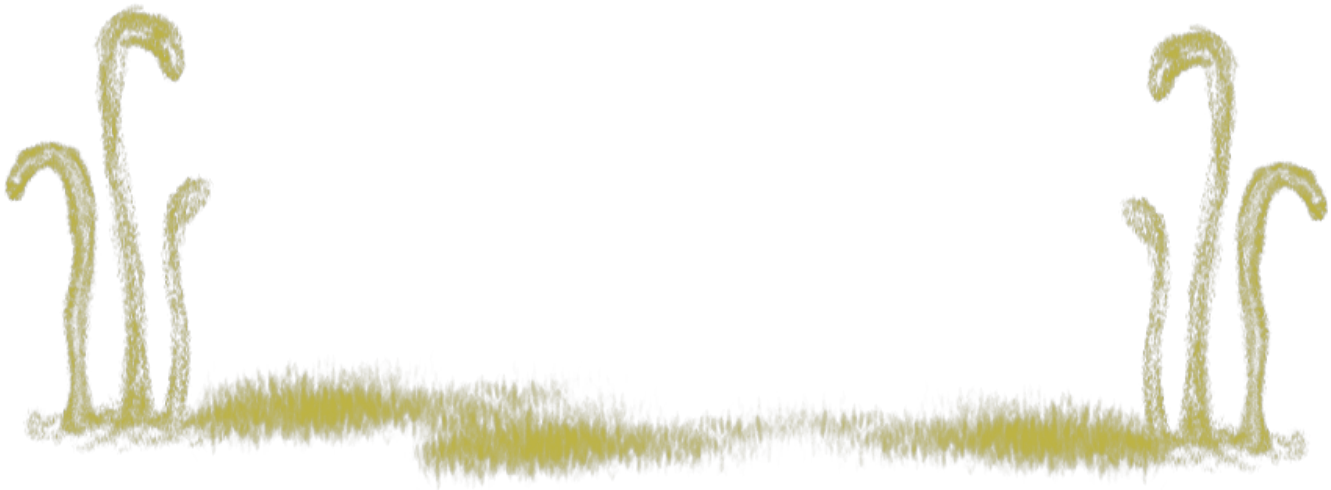
Résumez ensuite leurs réponses et enchaînez avec la présentation.

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

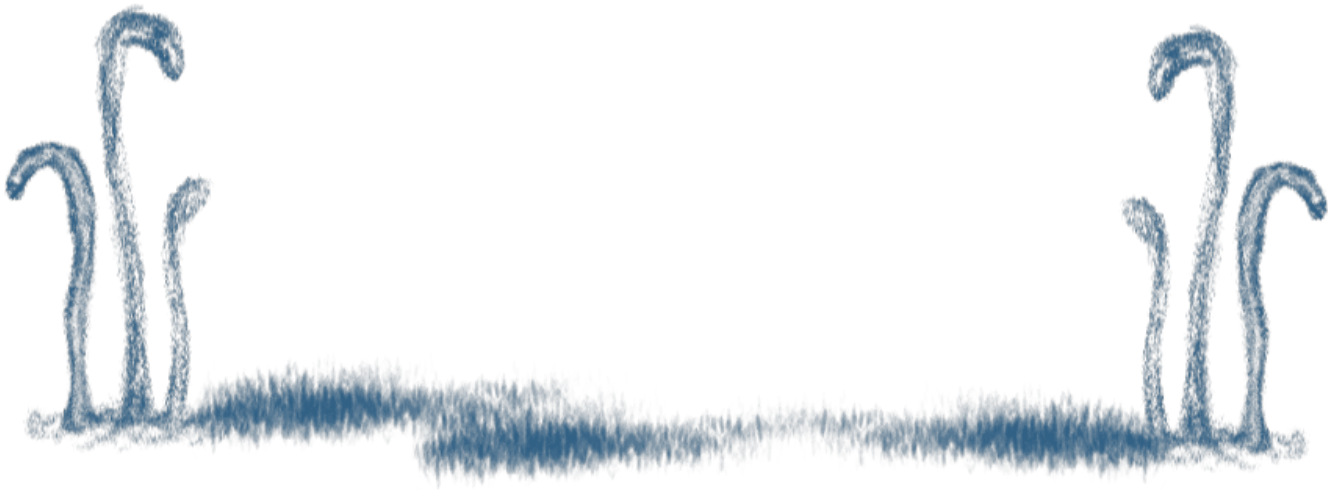
- Astuces, outils et guides pratiques pour des communications en ligne plus sécurisées : https://ssd.eff.org/fr
- Qu'est-ce le chiffrement? (MyShadow, en anglais) : https://myshadow.org/alternative-chat-apps#end-to-end-encryption-amp-perfect-forward-secrecy
- WhatsApp : voici les 5 meilleures messageries 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



Revision #4
Created 26 April 2023 01:05:00 by Kira
Updated 28 June 2023 20:04:40 by Kira