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

activ_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.

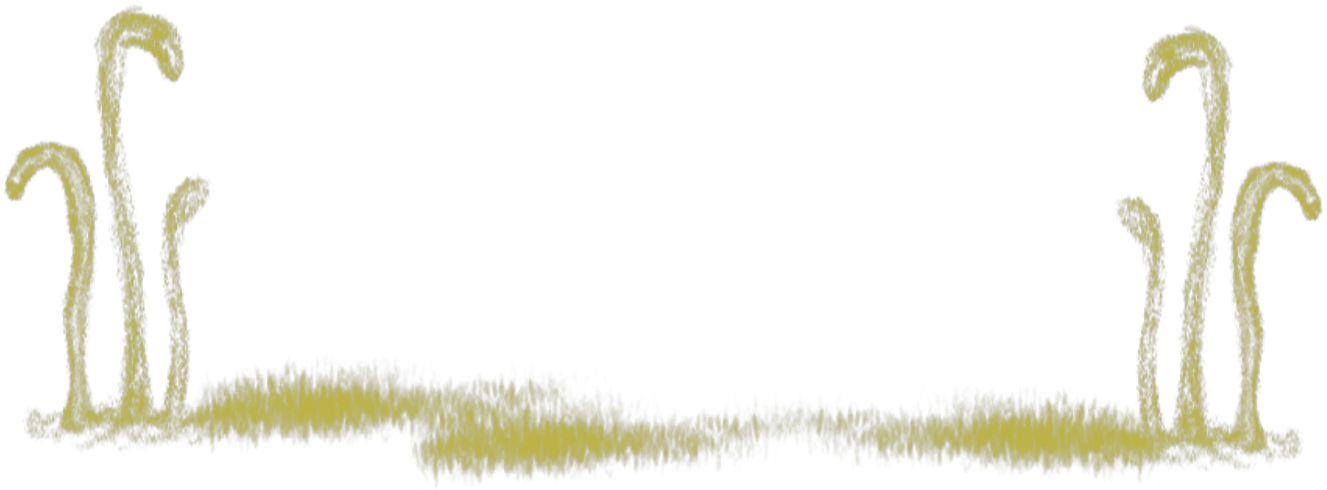
Quelques considérations : Est-ce que mon service mobile ou mon application chiffrent mes données en transit ? Est-ce que mes données sont chiffrées une fois stockées par le service mobile ? Est-ce que j'ai connaissances de situations où des opposants politiques ont pu accéder à ce genre de données ?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



Revision #5
Created 26 April 2023 01:03:04 by Kira
Updated 28 July 2023 15:04:34 by Kira