ACTIVITÉ - CE QUE TON SMARTPHONE SAIT DE TOI

SÉCURITÉ > 4.2 PROTÉGER LES DONNÉES PERSONNELLES ET LA VIE PRIVÉE

CONVIENT POUR	AGE	NIVEAU DE COMPÉTENCE	FORMAT	DROITS D'AUTEUR	LANGUE(S)
Chercheurs d'emploi, Elèves (école secondaire), Jeunes en décrochage scolaire, Tous publics	Adolescents, Adultes, Seniors	Niveau 1	Fiche d'activité	Creative Commons (BY-SA)	Français

Découverte de l’application Exodus qui permet d’identifier les pisteurs utilisés par chaque application installée sur les smartphones des participant.e.s.

Objectif général	Compétences
Temps de préparation pour l'animateur	moins d'une 1 heure
Domaine de compétence	4 - Protection de l’identité et des données personnelles
Temps requis pour compléter l'activité (pour l'apprenant)	0 – 1 heure
Nom de l'auteur	Nothing 2hide
Matériel supplémentaire	Smartphone Android - Paper boards ou tableau

Ressource originellement créée	Français

DÉROULÉ

1 Introduction

Cette activité courte permet de visualiser l'ensemble des trackeurs utilisés par les développeurs d'application mobile pour récupérer les données personnelles que nous produisons via nos smartphones.

En effet, nous utilisons tous des applications Android, jeux, applications utiles… Vous pouvez les télécharger et les installer depuis l'application Google play. Beaucoup d'applications sont également pré-installées par le constructeur de votre smartphone ou par votre opérateur si vous avez acheté votre téléphone par ce biais (news SFR, Tv Orange, etc.).

Vous l'avez remarqué, lorsque vous installez une application sur votre smartphone, celle-ci vous demande l'autorisation d'accéder à des fonctionnalités et données de votre téléphone : caméra, micro, mémoire, carnet d'adresses, etc. C'est la face visible de l'iceberg (qui n'est déjà pas belle, en quoi le jeu Golf Duck a-t-il besoin d'avoir accès à ma caméra et mes contacts ?).

Il existe également une face cachée de l'iceberg : toutes ces applications communiquent avec des services en ligne, parfois tout à fait légitimes (par exemple votre application météo a besoin de se connecter à un service en ligne qui lui permet de connaître le temps qu'il fera) mais parfois et même souvent beaucoup moins légitimes ! Tout ceci était invisible pour la majorité des utilisateur.rice.s sans connaissance technique avancée, puis Exodus est arrivé !

Exodus est une application dont l'objectif est de : *« lister les applications que vous avez installées depuis Google Play et de vous dire quels pisteurs sont utilisés pour chacune d'entre elles. L'application ne fait aucune analyse sur votre ordiphone mais va chercher les rapports disponibles sur la plateforme Exodus et ne contient aucun pisteur. »*

Conseil médiation :

Pour cette activité il est préférable que les participant.es utilisent leurs propres smartphones.

2 Déroulé

En amont de l'atelier, sur un tableau blanc ou un paper board, tracer un tableau avec :

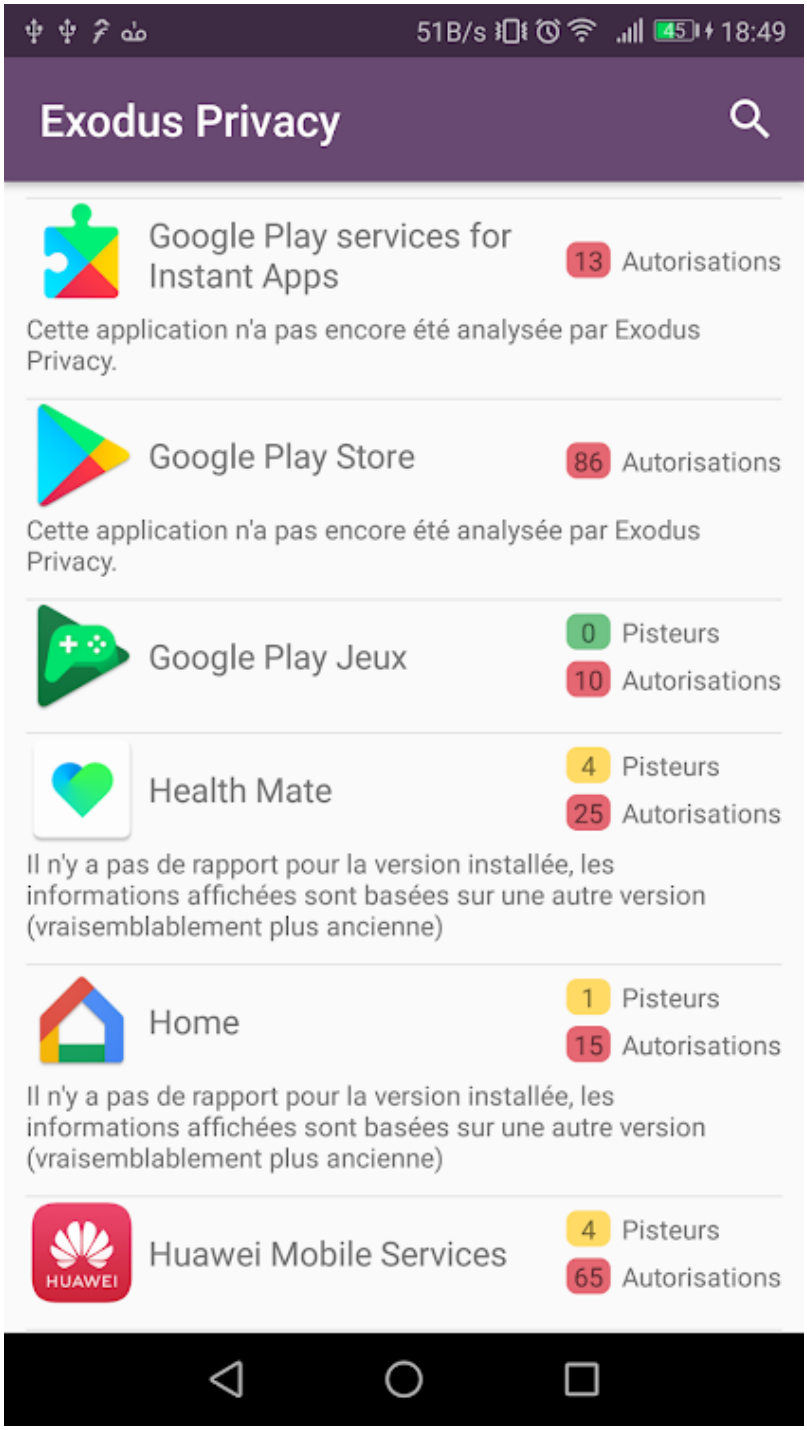
- 3 colonnes avec en entête Jaune | Rouge | Application
- et autant de lignes que de participant.e.s (ou écrire le prénom de chaque détenteur.rice de portable)

Cela va servir pour la suite de l'activité.

Faire installer aux participant.e.s l'application https://play.google.com/store/apps/details?id=org.eu.exodus_privacy.exodusprivacy ou dans Play Store leur faire chercher l'application Exodus Privacy.

Celle-ci est facilement repérable grâce à son logo :

Demander aux participant.e.s de lancer l'application. Celle-ci va lister les applications et afficher le rapport sous cette forme :

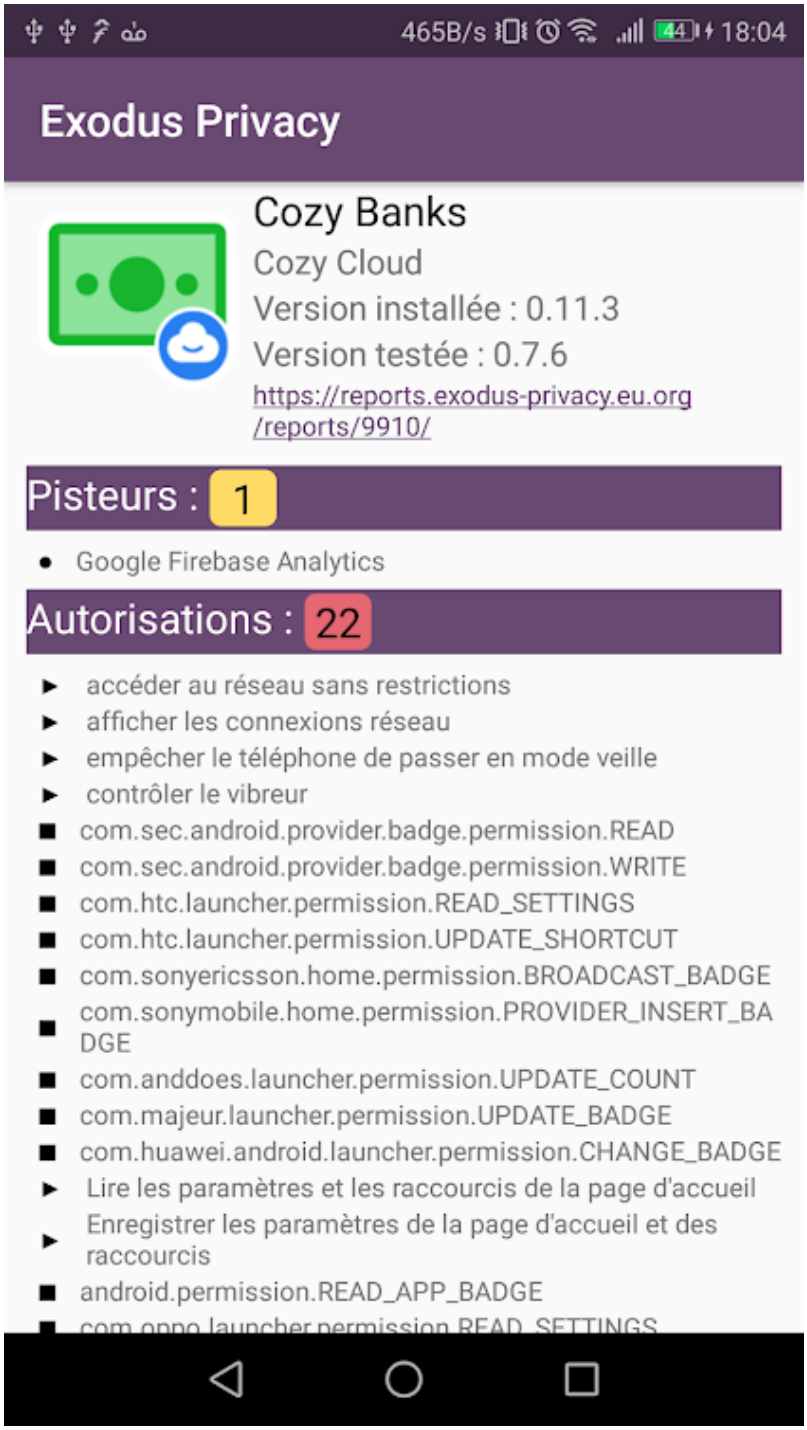


Demander aux participant.e.s de compter combien ielles ont de pisteurs (en jaune) en tout ou de permissions autorisée (en rouge) et noter *leur score* tableau en face de leurs prénoms ainsi que le nom

de l’application qui a le pire score.

Note à l’animateur.rice : Afin de ne pas mettre mal à l’aise les utilisateur.rice.s d’application de type rencontre en ligne ou autre il est préférable que chaque participant.e fasse cela à sa place et seul.e. On est là pour parler de vie privée, alors respectons la y compris pendant l’atelier !

Une fois le tableau rempli, demander aux participant.e.s de jeter un coup d’œil sur les détails en touchant les applications listées. Laisser 5 – 10 mn aux participant.e.s pour découvrir les applications qu’ielles ont aussi (installées et certainement oubliées):

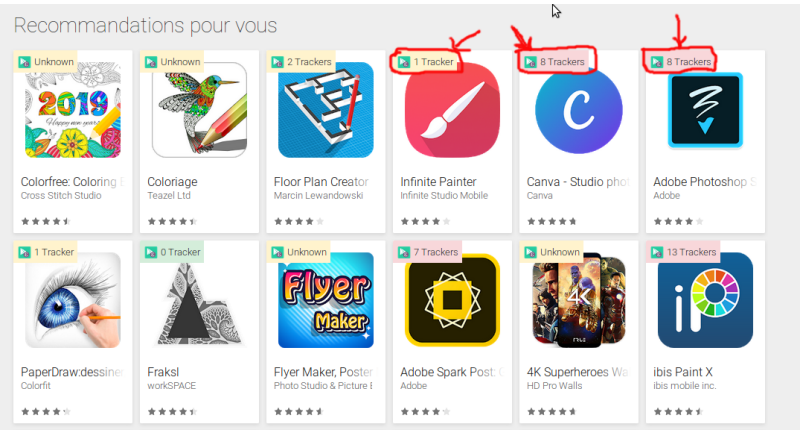


Leur demander alors s’ielles ont trouvé des applications particulièrement intrusives qu’ielles n’utilisent plus ou qui n’auraient pour elleux aucune utilité. Maintenant qu’ielles savent qu’ielles sont tracké.e.s et

qu'ielles ont les moyens de le savoir, vont-ielles changer leurs habitudes et être plus regardant.e.s sur les applications qu'ielles installent et sur les autorisations demandées.

Exodus donne la possibilité de vérifier le nombre de trackers et de permissions demandées par une application avant même de l'installer !

1. Le site https://reports.exodus-privacy.eu.org/fr/ permet de chercher directement une application déjà testée.
2. Il existe également une extension que vous pouvez installer dans votre navigateur : Exodify pour Firefox ou Google Chrome. Une fois installée, l'extension détectera automatiquement que vous vous rendez sur le site de Google Play et affichera le nombre de trackers pour chaque application dans la page courante comme ceci:



3 Pour conclure

Il est très compliqué de lutter contre les trackers / mouchards, c'est le prix à payer pour avoir des applications gratuites malheureusement. Les questions à se poser sont peut-être les suivantes :

- Puis-je faire confiance aux éditeur.rice.s de cette application qui vont avoir accès à mes données privées ?
- Ai-je vraiment besoin de cette application qui installe 32 mouchards ?
- Cela vaut-il le coup d'être tracké.e, se faire piller ses contacts, etc .. juste pour une application qui fait clignoter le fond d'écran avec des chatons tout mignons ?

À chacun.e de décider !