Atelier Smartphone et vie privée: Reprendre le contrôle 📱🔗

(Atelier pratique destiné aux débutant.es , animé par l'association root66.net)

Objectif :

Apprendre à reprendre le contrôle de son smartphone, améliorer sa vie privée et limiter le tracking des données.

Au delà de ces aspects , limiter la collecte de données sur son smartohone c'est aussi augmenter son autonomie en batterie

Mot de passe Wi-Fi :

À communiquer en début d'atelier

---

1. Contexte : Les dangers pour la vie privée

Types de collecte de données :

- **Collectes actives :** Traces intentionnelles laissées par l'utilisateur lorsqu'il surfe sur le web (ex. : cookies).
- **Collectes passives :** Traces non intentionnelles collectées sans consentement – fingerprinting du navigateur..applications (pisteurs, traceurs), capteurs.
  Traquent nos comportements numériques pour les revendre à des databrokers .

---

2. Diagnostic : Visualiser le tracking sur son smartphone

A. Traces laissées par le navigateur

1. **Tester la confidentialité de son navigateur :**
   - Lancer son navigateur sur son smartphone.
   - Aller sur https://coveryourtracks.eff.org/ et lancez le test.
   - Aller sur https://lehollandaisvolant.net/tout/tools/browser/
   - Installer l'extension lightbeam et naviguer de site en site pour visualiser l'ampleur des traces que l'on laisse sur le web
2. **Constat :**
   - Votre navigateur peut être facilement identifiable :
     - à cause des **cookies**
     - à cause du **fingerprinting (**empreinte unique*)

B. Identifier les applications les plus intrusives

1. **Installer Fdroid** le magasin d'applications libres avec ton navigateur va sur : https://f-droid.org/fr/

2. **Installer l'appli Exodus Privacy** :
    - **dans F-Droid** ou le playstore **,** dans la barre de recherche tape « exodus »
    - installer et ouvrir l'appli
3. **Analyse des applications :**
    - Utilisez Exodus Privacy pour visualiser les permissions et les pisteurs des apps
    - les applis avec le nombre de pisteurs indiqué en rouge sont à éviter absolument. Les applis de transport , de météo sont souvent truffées de trackers

=> éviter d'installer des applis lorsque cela est possible

4. **Solution :**
    - Remplacer les applications intrusives par des **raccourcis de navigateur**.
    - Raccourci meteo :
      - aller sur site meteofrance.com
      - « ajouter ajouter à la page d'accueil »

---

3. Actions et Solutions pour Améliorer sa Vie Privée

Quelques paramétrages de base :

Configuration du smartphone :

- **Vérifier et ajuster les autorisations des applications :**

  `Paramètres > Applications > Autorisations.`

- **Paramètres de géolocalisation :** Désactiver la localisation quand elle n'est pas nécessaire.
- **Désactiver la synchronisation et les sauvegardes automatiques** des services GAFAM and co
- **Réinitialiser l'identifiant publicitaire (AAID) :**
    - **Android 12 et plus :**

      `Paramètres > Confidentialité > Annonces > Supprimer l'identifiant publicitaire.`

    - **Android <12 :**

      `Paramètres > Google > Annonces > Désactiver personnalisation des annonces.`
      Source : Numerama

Applications alternatives respectueuses de la Vie Privée :

- **Store d'applications :**
    - **F-Droid** : magasin d'applications libres et open source.

Pour installer Fdroid , télécharger l'application sur le site officiel.
- Appuyer sur le bouton TELECHARGER F-DROID.
- une fois le téléchargement terminé, appuyer sur la notification pour lancer l'installation de l'application
- cocher *Sources Inconnues* car il faut lui dire au sytéme d'accepter une app, un fichier APK autre que ceux du play$tore

Une fois Fdroid installé, tu pourras récupérer toutes les applis libres
Lance Fdroid et fait la maj en tirant vers le bas avec ton doigt.

Voici une liste non exhaustive des applications conseillées pour améliorer ta vie privée

- **Navigateur :**
    - sur Fdroid, **télécharger Firefox** (fennec ou mull) + extension **uBlock Origin**
    - Remplacer le moteur de recherche Google par **DuckDuckGo**
    - Paramétrer sa page d'accueil
- **Clients mail :**
    - **Thunderbird**, **K-9 Mail** .
    - Alternatives fournisseurs mails : **Tutanota**, **ProtonMail**...(éviter Gmail).
- **Messagerie :**
    - **Signal** au lieu de WhatsApp ou Messenger.
    - **Silence** pour les sms
- **Multimédia :**
    - **NewPipe** (YouTube sans tracking), **VLC** pour les vidéos.
- **Clavier :**
    - Remplacer par exemple par **Simple Keyboard**.

---

4. Faire le Ménage : Supprimer les Applications Indésirables (Bloatware)

Impossible de désinstaller certaines applications préinstallées par le constructeur ou google.
Le menu est grisé. Il existe un moyen pour les supprimer grâce à linux et adb.

⚠️ ces manipulations sont à réaliser avec une extrême précaution

cas pratique : supprimer le navigateur chrome ou le lecteur youtube

Méthode 1 : Suppression manuelle avec `adb`

1. **Activer le mode développeur :**

```
Paramètres > Système > À propos du téléphone > Appuyer 7 fois sur le
numéro de build.
```

2. **Activer le débogage USB :**

```
Paramètres > Options développeur > Activer le débogage USB.
```

3. **Connecter le smartphone au PC avec un câble USB.**
4. **Lister les applications Google :**

```
adb devices
adb shell pm list packages | grep google
```

5. **Désinstaller une application (ex. : YouTube) :**

```
adb shell pm uninstall --user 0 com.google.android.youtube
```

6. **Désactiver une application sans la désinstaller :**

```
adb shell pm disable-user --user 0 com.google.android.youtube
```

Liens utiles :

- Libérer son Android avec ADB
- Debloater tuto wikilibriste
- Désinstaller les spywares sur Android

Méthode 2 : Utiliser un logiciel Universal Android Debloater (UDA)

1. **Télécharger** UDA **:**
    - **Linux :** Lien de téléchargement
2. **Exécuter** le logiciel sur PC pour nettoyer les applications.

---

5. Installer un Android Respectueux de la Vie Privée

Pour aller plus loin :

il existe des images (rom) android qui permettent de remplacer le système préinstallé par le constructeur du smartphone. Ces images sont « dégooglisées » et ont été débarrassées des applications intrusives (bloatwares).

Nous conseillons principalement :

- lineageOS
- grapheneOS

E/os est un lineageOS amélioré et qui propose des services supplémentaires. Pour les débutants c'est sans doute le moyen le plus facile pour commencer à utiliser un android « propre ».

démo d'installation :

L'installation n'est pas forcément aisée pour un néophyte. Les procédures peuvent varier en fonction du modèle du smartphone. C'est pourquoi Root66 propose des « **smartphone party** » pour accompagner les utilisateurs et utilisatrices dans la libération de leur téléphone .

Néanmoins, on peut saluer l'initiative de E/OS pour avoir mis à disposition un programme d'installation qui simplifie grandement les opérations . Il n'est valable que pour certains modèles :

/e/OS :

1. **Installer Easy Installer :**

   ```
   sudo snap install easy-installer --channel=latest/beta
   ```

2. **Suivre les instructions pour installer /e/OS sur votre appareil.**

Conclusion : Reprendre le contrôle

- **Résumé des actions :**
  - Diagnostiquer le tracking.
  - Remplacer les applications intrusives.
  - Configurer le smartphone pour limiter le tracking.
  - Faire le ménage des bloatwares.

🎯 Objectif final :

Les participant.es repartent avec un smartphone configuré pour protéger et améliorer leur vie privée ,des outils pour rester maîtres de leurs données et des conseils pour être autonomes.

Glossaire

fingerprinting :
une technique d'identification qui analyse les caractéristiques techniques de ton appareil pour créer un profil unique d'un utilisateur. Au lieu de stocker des informations sur l'appareil de l'utilisateur comme le font les cookies, le fingerprinting collecte des données telles que la version du système d'exploitation, la résolution d'écran, les polices installées,la langue et bien d'autres éléments qui, ensemble, permettent d'identifier de manière **unique** un navigateur ou un appareil.

Bonus :
Comment vérifier si son mail se trouve dans une base de données qui a fuité ?
https://haveibeenpwned.com/