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 en limiter le pistage de ses données persos.

- Comprendre le tracking et le visualiser
- Configurer son téléphone pour limiter la collecte
- Installer des alternatives
- Commencer à nettoyer

Disclaimer :

Aujourdhui propose cet atelier qui est dans la continuité de la conférence smartphone et vie privée . Passer de la théorie à la pratique.

Des manipulations vont être proposées pendant l'atelier

- Vous pouvez suivre, regarder ou tester : rien n'est obligatoire,
- On avance étape par étape, chacun à son rythme,
- On ne pourra pas tout voir aujourd'hui - niveau débutant.e

À savoir :

- Selon les **modèles de smartphone**, les menus et les manipulations peuvent varier
- **atelier participatif** n'hésitez pas aussi à vous entraider ou à solliciter notre team root66 durant l'atelier

👉 Si ça vous intéresse, l'association propose aussi des permanences pour aller plus loin et vous accompagner

1. Intro / contexte : pourquoi votre smartphone vous piste (5min)

Ya ce que vs donnez volontairement… et ce que le téléphone prend tout seul à votre insu

- Collecte active (cookies first, comptes google, formulaire ..) - consentement
- Collecte passive (via les sites et applications , fingerprinting, capteurs : gps ,wifi , bt)

👉 modèle économique = revente de données / ciblage profil publicitaire

Si c’est gratuit, c’est vous le produit
Même quand vous faites attention, il reste beaucoup de collecte invisible

=> Maintenant voir ça concrètement sur vos téléphones

2. 🔎 Diagnostic : voir le tracking (35 min)

A. 🌐 Navigateur (15 min)

Exercice

- https://amiunique.org/fingerprint
- https://coveryourtracks.eff.org/
- https://lehollandaisvolant.net/tout/tools/browser/

Débrief

- Cookies tiers
- fingerprinting

  ...

Un bon navigateur libre + une extension de blocage = déjà une énorme réduction du tracking.

Mais le tracking ne vient pas que du web…

B. Applications (15 min)

Installer l’application Exodus Privacy depuis le store (google ou fdroid)
ou aller sur le site

Observer

- Trackers / pisteurs
- permissions

les pires applications = les préinstallées
(ex : Gapps, applis constructeurs, meteo , transports, reseaux sociaux

- voir permissions d’apps comme Youtube ou meteo france

=> Et même sans ouvrir d’appli ...

C. DNS (démo) (5 min)

👉 démonstration Pi-hole
Observer **requêtes dns** smartphone :

- au boot
- au lancement d'une appli

Même quand vous ne faites rien, votre téléphone parle dans votre dos !

Bonne nouvelle : on peut déjà agir facilement et limiter toute cette collecte de datasS

---

3. Actions concrètes (35 min)

A . Paramétrer les autorisations des applications

→ gestionnaire d'autorisations
ex : désactiver localisation , micro , acces contacts

B. Réduire les applications inutiles (5 min)

👉 Bonne pratique :

éviter d'installer une application quand un site web suffit

Exemple météo : créer le raccourci

- https://meteofrance.com
- "Ajouter à l'écran d'accueil"

Moins d'applications = moins de tracking.
++ d'applications libres = moins de tracking

C. Installer des alternatives libres (15 min)

👉 via : télécharger et installer le magasin d'applis libres

Les indispensables

Navigateur

- Fennec , Mull, Duckduckgo privacy browser...
- uBlock Origin
- DuckDuckGo

...

Messagerie

- Signal

Mail

- Thunderbird

Se déplacer :

- comaps

Autres – liste non exhaustive

- Calendrier : **Etar**
- Gestionnaire de mot de passe : **keepass**
- lecteur youtube : **NewPipe**
- lecteur multimédia : VLC
- clavier : Simple Keyboard / Heliboard
- Saracroche (filtrer les appels indésirables)
- prendre des notes : joplin
- Nextcloud
- Shelter

…

Démo :
→ Trouver des alternatives grâce à l'app **LibreFind**

Dernier recours si tu es obligé d'installer des applications du playstore ? (ex : applis bancaires)
→ installe l'app **Aurora**

permet de télécharger sur le playstore sans être pisté

D. 🔧 Réglages essentiels (15 min)

🔎 1. Autorisations des applications

☐ Ouvrir : Paramètres → Confidentialité → Gestionnaire d’autorisations
☐ Vérifier accès :

- ☐ Localisation
- ☐ Micro
- ☐ Caméra
- ☐ Contacts

  ☐ Retirer toutes les autorisations inutiles

📍 2. Localisation

☐ Désactiver la localisation si inutile
☐ Sinon : activer uniquement “pendant l’utilisation”
☐ Privilégier la **position approximative**

🎙️ 3. Micro & Caméra

☐ Autoriser uniquement pour les apps essentielles
☐ Refuser accès permanent

📢 4. Publicité & tracking

☐ Paramètres → Google → Annonces
☐ ☐ Supprimer / réinitialiser l’identifiant publicitaire
☐ ☐ Désactiver la personnalisation des annonces

🌐 5. Compte Google

☐ Aller sur : myaccount.google.com
☐ ☐ Désactiver historique des positions
☐ ☐ Désactiver activité Web & Apps
☐ ☐ Supprimer anciennes activités

📊 6. Tableau de bord confidentialité

☐ Paramètres → Confidentialité → Tableau de bord
☐ Vérifier :

- ☐ quelles apps accèdent au micro
- ☐ à la caméra
- ☐ à la localisation

  ...

DNS privé :

Exemples de dns éthiques que l'on peut utiliser sur android pour améliorer vie privÉe:

- dns.mullvad.net
- dns.quad9.net
- adblock.dns.mullvad.net

Pour celles et ceux qui veulent aller plus loin…

---

4. 🧹 Niveau intermédiaire : nettoyage (15 min)

Supprimer les apps préinstallées

👉 problème : bloatwares

activer le debogage USB

Démo ADB

```
adb devices
adb shell pm list packages | grep google
adb shell pm uninstall --user 0 com.google.android.youtube
```

Alternatives via un logiciel

- à installer sur pc : Universal Android Debloater
- application android : **Canta debloater** (dispo sur playstore ou ici) – nÉcessite service shizuku

⚠️ ces manipulations sont à réaliser avec une extrême précaution

5. Aller plus loin : déGAFAMiser (10 min)

Services alternatifs

👉 CHATONS
👉 Framasoft

mail, visio, synchro celendrier, contacts, fichiers, pad etc

Android alternatifs dÉgooglisÉs

- LineageOS
- GrapheneOS
- /e/OS

  ...

Notre conseil pour débutant.es :

- Acheter smartphone préconfiguré sur murena.org
avec un système et des services degoolisés : fairphone + eos

- Tester avec un ancien téléphone ou acheté sur LBC pour installer E/os
→ Se faire accompagner lors de smarphone party chez root66 par exemple :-)

CONCLUSION (5 min)

Ce qu'on a vu à travers cet atelier :

- observer et comprendre le tracking
- agir concrètement avec bonnes pratiques et outils
- avancer progressivement , à son rythme
- smartphones party ...

Ressources :

- Diaporama smartphone et vie privée:
https://tutox.fr/wp-content/uploads/2026/SmartphoneEtViePrivee_benzo_20260404_final.pdf

- Vérifier les trackers d’ une application:
https://reports.exodus-privacy.eu.org/fr/

- Recommandations de la cnil :
https://www.cnil.fr/fr/applications-mobiles-les-recommandations-de-la-cnil

- Participer à une install party :
https://root66.net/
https://www.electrocycle.co/

- Trouver des alternatives libres et Éthiques :
Chatons
Framasoft
Alternativeto.net

- Guide pratique options confidentialité Android :
https://ssd.eff.org/fr/module/guide-pratique-decouvrir-les-parametres-de-confidentialite-et-de-securite-android