

100%
PRATIQUE

[ASTUCES]
Fonctions cachées

[TV & VIDÉOS]
Passez à l'illimité

[ROM CUSTOMS]
Tout personnaliser !

3,50€
seulement

0%
PUBLICITÉ

iPhone



Android



BEST-OF
APPLIS
SECRÈTES
& interdites

80 HACKS

POUR VOTRE

SMARTPHONE

**ROOT &
JAILBREAK**
DÉBRIDEZ
& DOPEZ
votre mobile !

PROTECTION

- » Êtes-vous espionné ?
- » Les meilleurs antivirus gratuits
- » Cacher ses dossiers, SMS, navigation, appels, contacts, etc.
- » Le Guide Anti-vol !

HACKING
Prenez le
CONTRÔLE!



EN PARTENARIAT AVEC

LES CAHIERS DU HACKER
PIRATE
[INFORMATIQUE]

➤ HACKING

6

ROOT & JAILBREAK :

Introduction

10

Le **JAILBREAK** facile

12

ROOTEZ facilement
votre appareil Android

18

Le contrôle à distance
avec **AIRDROID**

22

Communiquez
sans réseau avec
FIRECHAT

28

WIFI MAP : toujours
un hotspot sous la main

30

OVERCLOCK : un
portable à pleine
puissance

32

DSPLOIT : testez et
sécurisez votre réseau

➤ PROTECTION

41

DOSSIER ANTIVOL :

que faire
pour se protéger ?

48

BOXCRYPTOR :

un cloud chiffré

52

AVAST ! SECURELINE :

un VPN efficace

54

Un mot de passe principal
avec **DASHLANE**

56

SECRECY : votre coffre fort
à fichier

58

IMSI CATCHER : êtes-vous
surveillés ?

60

Empêchez les applis
d'accéder à votre
compte **GOOGLE+**

62

ORBOT, le Tor version
Android !

65

MOUCHARDS sur mobile :
comment ça marche et comment
s'en débarrasser ?

70

Faites le ménage avec **CCLEANER**

72

Restaurez vos applis avec **APPS
BACKUP & RESTORE**

74

Verrouillez l'accès à vos applis avec
APPLOCK

76

SMSSECURE : Chiffrez vos SMS

MULTIMÉDIA

86

µTORRENT pour
télécharger sur mobile

88

Le Netflix du pauvre :
POPCORN TIME

92

SOUS-TITRES sur mobile :
Nos solutions

MATOS

98

**NOTRE SÉLECTION
DE MATÉRIELS**

LES DOSSIERS DU Pirate

N°4 – Juillet-Septembre 2015

Une publication du groupe ID Presse.
27, bd Charles Moretti - 13014 Marseille
E-mail : redaction@idpresse.com

Directeur de la publication :

David Côme

Rick Deckard : Benoît BAILLEUL

Les Nexus-6 : Michaël Couvret, Yann
Peyrot, Thomas Povéda, Pierre Cobinais

J.F Sebastian : Sergueï Afanasiuk

Pris : Stéphanie Compain

Zhora : Karima Allali

Imprimé en France par

/ Printed in France by :

Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : en cours

«Pirate» est édité par SARL ID Presse,
RCS : Marseille 491 497 665
Capital social : 2000,00 €
Parution : 4 numéros par an.

La reproduction, même partielle, des
articles et illustrations parues dans «Pirate
Informatique» est interdite. Copyrights et
tous droits réservés ID Presse. La rédaction
n'est pas responsable des textes et photos
communiqués. Sauf accord particulier, les
manuscrits, photos et dessins adressés à la
rédaction ne sont ni rendus ni renvoyés. Les
indications de prix et d'adresses figurant
dans les pages rédactionnelles sont données
à titre d'information, sans aucun
but publicitaire.

CHEZ VOTRE
MARCHAND DE JOURNAUX
**LES PIRATES CRYPTENT,
NOS LECTEURS DÉCRYPTENT !**

WI-FI,
ANONYME,
MOBILES,
HACKING,
ENCODAGE,
ANTIVOL,
CRYPTAGE,
MOTS
DE PASSE,
SURVEILLANCE

+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER
PIRATE
[INFORMATIQUE] // 25

LE GUIDE
DU HACKER
**PRENEZ
LE
CONTRÔLE !**

100% HACKING
AVEC CD GRATUIT
➤ PLUS DE 50 FICHES
PRATIQUES



**0% PUB
0% CENSURE**



KEYLOGGER
ESPIONNEZ
QUI ÉCRIT QUOI
SUR VOTRE CLAVIER

SURVEILLANCE
BLOQUEZ GOOGLE,
LA NSA ET LE
GOUVERNEMENT

TÉLÉCHARGE
LE GUIDE PRATIQUE
POUR TÉLÉCHARGER
SUR SEEDBOX

+ CD GRATUIT PACK 100% PIRATE

HACKING

6

ROOT & JAILBREAK :

Introduction

10

Le **JAILBREAK** facile

12

ROOTEZ facilement votre
appareil Android

18

Le contrôle à distance
avec **AIRDROID**

22

Communiquez sans réseau
avec **FIRECHAT**

28

WIFI MAP : toujours un hotspot
sous la main

30

OVERCLOCK : un portable à
pleine puissance

32

DSPLOIT : testez et sécurisez





ROOT & JAILBREAK

- LES DIFFÉRENCES ET LES AVANTAGES -

POSSEURS D'APPAREIL MOBILE SOUS iOS OU ANDROID VOUS AVEZ SANS DOUTE DÉJÀ ENTENDU PARLÉ DE ROOT OU DE JAILBREAK. QU'IL S'AGISSE DE TABLETTE OU DE TÉLÉPHONE, NOUS AVONS DÉCIDÉ DE FAIRE UN RÉCAPITULATIF DES AVANTAGES ET DES INCONVÉNIENTS DE CES TECHNIQUES...



Il arrive souvent que les sites ou les revues spécialisés en nouvelles technologies fassent l'amalgame entre le root Android et le Jailbreak iOS (iPhone, iPad, etc.) Même s'il s'agit dans les deux d'une modification du système, les deux techniques n'ont pas le même but et ne s'adressent pas aux mêmes types d'utilisateurs. Nous verrons que le jailbreak sur iPhone permet principalement d'installer des applications non approuvées par Apple que le root Android est plus un outil pour bidouilleur...

ANDROID, BASÉ SUR LINUX

Android est basé sur un noyau Linux. Les systèmes de ce type permettent de créer des profils élargissant les droits d'accès des utilisateurs. Il est non seulement possible d'y accéder en mode «super-utilisateur» (SU ou root) afin d'exécuter des tâches jusque-là interdites, mais certains programmes peuvent aussi utiliser ce mode SU pour proposer des fonctionnalités avancées. Pour pouvoir profiter de ce mode sur votre téléphone, il est nécessaire d'y apporter quelques modifications, c'est ce qui s'appelle «rooter» son téléphone. Notez qu'il n'y a aucun lien entre le fait de rooter son téléphone et le

piratage. Il s'agit d'une modification légale et encouragée par Google. Attention certains constructeurs sont peu enclins à autoriser le root et stipulent refuser les appareils modifiés en SAV. Heureusement la manipulation est réversible...

COMMENT?

Nous n'allons pas présenter de méthode particulière pour rooter son téléphone sous Android car le procédé est différent pour chaque appareil. Néanmoins, nous vous ferons découvrir dans les pages suivantes plusieurs solutions. Par fois il faudra bancher votre machine sur votre PC alors que pour d'autres, il faudra placer un fichier directement sur la carte SIM puis faire une mise à jour. Ici, Google est votre ami et si nos méthodes ne sont pas compatibles avec votre appareil, vous pourrez sans problème trouver une méthode clé en main en tapant «Galaxy 4 root» ou «root HTC M8» par exemple.



ROOT ET JAILBREAK SONT DES MODIFICATIONS QUI NE DEMANDENT PAS DE COMPÉTENCES PARTICULIÈRES

IL EST LIBRE ANDROID

Le jailbreak sur iPhone permet principalement d'installer des applications non approuvées par Apple (voire même piratées) alors que sur Android, il suffit de cocher une case pour y parvenir (**Paramètres>Sécurité>Sources inconnues**).



PRATIQUE



LE ROOT POUR QUOI FAIRE?

01 > CHANGER LE SYSTÈME POUR UNE «CUSTOM ROM»

Une fois que vous avez rooté votre téléphone, les programmes qui utilisent cette fonctionnalité pourront faire leur œuvre, mais les performances



de votre appareil ne seront pas plus avancées. Pour un changement en profondeur, il faudra changer la ROM: une version modifiée du système permettant d'ajouter de nouvelles fonctionnalités ou d'améliorer les performances (overclocking, etc.) Il est même possible de jongler entre plusieurs ROM grâce à un logiciel comme ROM Manager.
Lien: <http://tinyurl.com/brdwuru>

02 > SAUVEGARDER SES APPLICATIONS

Pas facile de faire une sauvegarde de tous les éléments de votre téléphone surtout lorsque vous êtes habitué à installer des dizaines d'applications

par semaines. En cas de changement de téléphone, il est possible de faire une sauvegarde avec un logiciel comme Titanium Backup. Non seulement il gère tous types de données (SMS, contacts, préférences, multimédia), mais il permet aussi de «geler» certaines applications ou de les «déplacer» sur une carte SD.

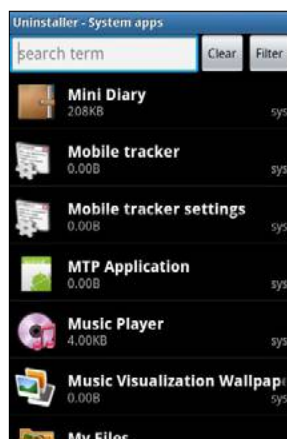
Lien: <http://tinyurl.com/kespfnh>



03 > DÉINSTALLER LES APPLICATIONS INUTILES

Si vous n'utilisez jamais les applications du constructeur (Samsung Apps, etc.) ou de votre opérateur (SFR truc, Orange machin-chose, etc.) vous pouvez vous en débarrasser avec un téléphone rooté. Vous gagnerez de la place sur votre bureau et dans la mémoire de votre appareil. Essayez Root Désinstallateur sur le Play Store!

Lien: <http://tinyurl.com/c7mkfp5>

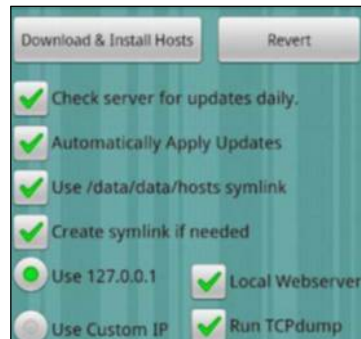




04 > SUPPRIMER LA PUB

La publicité sert à rémunérer les développeurs qui font le choix de proposer des applications gratuites. Le problème c'est qu'avec les limitations des forfaits, vous devez sacrifier beaucoup de bande passante pour afficher ces pubs, même avec des applications ne nécessitant pas de connexion! Il existe des solutions ne nécessitant pas de root mais elles sont moins efficaces que AddFree, par exemple, qui supprime tout simplement la pub et les dépassements de forfait qui vont avec...

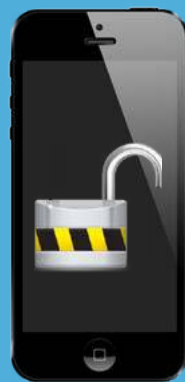
Lien: <http://adfree.bigtincan.com>



➔ LIBÉREZ IOS!

Le jailbreak d'un appareil sous iOS permet d'obtenir un accès au système, comme pour le root Android (même si pour ce dernier, la nature même de Linux fait que les possibilités sont plus étendues). Mais ce qui motive plus les utilisateurs c'est qu'en plus, ils pourront installer des applications n'ayant pas été approuvées par Apple ainsi que des éléments graphiques alternatifs. Il s'agit en fait de hacker l'OS de la machine pour accéder à des fonctions et programmes qu'Apple n'autorise pas à l'origine. Car l'iOS est un système fermé et Apple impose des

bornes aux différents développeurs qui veulent programmer des applis sur la machine. Après un jailbreak, il devient possible de changer le thème, d'installer des logiciels que ne viennent pas forcément de l'AppStore, d'utiliser le Bluetooth pour transférer ses fichiers et se connecter à un GPS externe. Il est aussi possible d'utiliser son iPhone comme une unité de stockage sans passer par un logiciel payant ou émuler des consoles de jeux. Il existe même des plates-formes dissidentes comme Cydia ou Icy qui proposent des milliers de logiciels se passant de l'approbation d'Apple.



UN JAILBREAK QUI SERT LE PIRATAGE ?

Enfin certains utilisateurs sont attirés par la possibilité de pirater les applications puisqu'avec un téléphone ou une tablette jailbreakée il est possible de se passer de l'Apple Store et télécharger des programmes non signés sur les réseaux P2P. Le jailbreak n'est donc pas une technique encouragée par Apple puisqu'elle s'appuie sur des failles du système que des hackers utilisent pour proposer des méthodes. Ces dernières varient selon la version du système d'exploitation iOS et selon le modèle. Pour y voir plus clair, nous vous donnerons dans les pages suivantes différentes pistes pour réaliser cette manipulation selon votre appareil.



JAILBREAK D'IOS : POURQUOI ET COMMENT ?



ON ENTEND PARLER DE CETTE TECHNIQUE UN PEU PARTOUT : AU BUREAU, DANS LES COURS DE RÉCRÉ ET MÊME DANS LES MÉDIAS «GÉNÉRALISTES». LE JAILBREAK CONSISTE EN FAIT À OUTREPASSER LES RESTRICTIONS DU SYSTÈME D'EXPLOITATION MAISON D'APPLE. À VOUS LA PERSONNALISATION DES ICÔNES, L'INSTALLATION DE LOGICIELS NON AGRÉÉS ET ENCORE PLEINS D'AUTRES CHOSSES...

À la rédaction nous n'aimons pas trop les appareils «figés». Inutile de préciser que les produits Apple font partie du lot : impossibilité de paramétrer comme on le désire, de bidouiller la bête ou même d'installer des logiciels qui n'ont pas été «signés» par la maison mère. Heureusement, le Jailbreaking vient un peu égayer tout ça et puisque c'est légal, pourquoi ne pas tenter l'expérience ?

JAIL QUOI ?

Le jailbreaking consiste en fait à casser (break) la prison (jail) construite autour de l'iPhone. Et puisque la politique d'Apple est la même pour toutes ses productions, il est aussi possible de «jailbreaker» les iPod Touch et les iPad. Il s'agit en fait de hacker l'OS de la machine pour accéder à des fonctions et programmes qu'Apple n'autorise pas à l'origine. Il est par exemple

possible de de personnaliser l'interface, d'installer des logiciels que ne vienne pas forcément de l'AppStore, d'utiliser son iPhone comme une unité de stockage sans passer par un logiciel payant et se connecter à un GPS externe. Il est aussi possible d'utiliser son iPhone comme une unité de stockage sans passer par un logiciel payant ou émuler des consoles de jeux (Game Boy Advance, NES, N64, etc.)



Un très bon point de départ pour les utilisateurs débutants



Pas toujours à jour avec certains types d'appareils





JAILBREAK WIZARD : CHACUN SA SOLUTION !

PRATIQUE



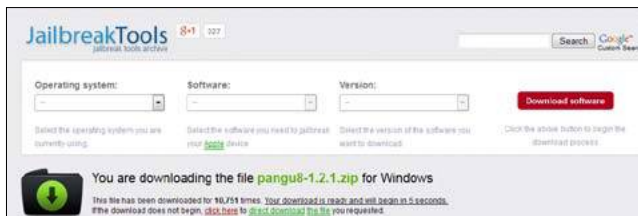
01 > LE SITE

Commencez par vous connecter au site et cliquez sur le modèle de votre appareil dans **iDevice**. Sélectionnez ensuite le modèle précis et la version de votre iOS. Pour connaître cette information, il suffit de faire **Réglage > General > Information > Version** sur votre machine. BaseBand permet d'opérer un désimlockage (débloquage pour tout type d'opérateur). Vous trouverez cette information dans **Réglage > General > Information > Prog du modem**. Dans **OS**, mettez Windows si c'est votre cas.



02 > SUR MESURE!

Si votre version est trop récente, le site vous le dira immédiatement. Dans le cas contraire, le site vous proposera de télécharger le meilleur outil pour votre cas personnel. Ici il faudra télécharger et installer **Pangu8 v1.2.1**. Suivez ensuite les instructions du logiciel. Bravo votre appareil est jailbreaké et vous aurez l'intégralité des applications interdites depuis l'icône Cydia...



LE JAILBREAK INTERDIT ?

Même s'il n'est pas interdit de jailbreaker son appareil, il est bien sûr interdit d'utiliser cette manipulation pour voler les auteurs d'applications. Mais pour Apple, qu'il soit pour pirater des programmes ou non, le jailbreaking n'est pas autorisé. Selon le constructeur, «*ces techniques, largement généralisées, font appel à des modifications non autorisées du chargeur d'amorçage et du système d'exploitation, ce qui conduit à une violation de notre copyright*». En effet, les logiciels qui permettent cette manœuvre contiennent des pans de code qui appartiennent à la société. Apple a donc décrété que l'opération empêchera la garantie de fonctionner.



INFOS [**KINGO ROOT**] Où le trouver ? [www.kingoapp.com]

[**SUPERSU**] Où le trouver ? [<https://goo.gl/4lwbmP>]

[**ROOT CHECKER**] Où le trouver ? [<https://goo.gl/Lg1lb4>]

Difficulté :

ROOTEZ FACILEMENT UN APPAREIL ANDROID

NOUS AVONS VU LES AVANTAGES DU ROOT DANS LES PAGES PRÉCÉDENTES, NOUS ALLONS MAINTENANT VOUS DONNER LES MEILLEURES PISTES POUR PASSER À L'ACTION. ET TANT QUE NOUS Y SOMMES, NOUS VERRONS AUSSI LES PRINCIPALES CUSTOM ROM ET COMMENT CARRÉMENT CHANGER VOTRE SYSTÈME...



Autrefois assez complexe, le root n'est plus vraiment un obstacle infranchissable, même pour un utilisateur débutant. Grâce à Kingo ROOT vous allez pouvoir rooter la plupart des téléphones du marché en quelques clics. Il est possible de passer par un logiciel sous

Windows, de brancher le téléphone ou la tablette en USB et de suivre les instructions à l'écran. Mais vous pourrez aussi tenter la méthode sans ordinateur avec un fichier APK à installer. Bien sûr nous vous proposons deux autres méthodes tout aussi simples (voir encadré) pour contenter tout le monde.



HACKING

Root & ROM Custom

Mais si jamais votre appareil ne veut rien savoir, la seule solution sera de «googler» votre problème avec quelque chose du genre «LG L7 root» ou «root Huawei P7» par exemple.

UN SUPER UTILISATEUR !

Une fois votre appareil rooté, à vous les multiples avantages du «super user» (enlever les pubs, désinstaller des applications normalement indéboulonnables, etc.), mais aussi les Rom Custom. Ces systèmes alternatifs sont basés sur les versions d'Android standards tout en apportant des modifications graphiques ou des fonctionnalités très sympas. Les Custom ROM sont donc des sortent de déclinaisons d'Android comme cela existe dans le monde Linux. Comme pour le root, il n'existe pas de méthode universelle : Google est ici votre meilleur ami. Sachez néanmoins que la plupart du temps il faudra débloquent le bootloader (le premier programme qui se charge lorsque vous allumez votre téléphone), sauvegarder la ROM d'origine puis charger la nouvelle avec le pack d'application Google (pour avoir accès au Play Store par exemple). Si vous aimez le changement, nous vous conseillons



CyanogenMod
en train de
s'installer
sur un Sony
Xperia S...

d'utiliser Rom Manager pour jongler plus facilement avec vos ROM. Attention, même si c'est très rare, une mauvaise manipulation peut rendre inutilisable votre téléphone...



POURQUOI NE PAS TIRER LE MAXIMUM DE VOTRE MATÉRIEL ?

ROOT OBLIGATOIRE POUR INSTALLER UNE ROM CUSTOM ?

Pour s'installer sur un appareil Android, une ROM Custom n'a pas forcément besoin d'un accès au root. Si vous avez installé un mode Recovery alternatif (ClockWorkMod par exemple) vous pouvez installer n'importe quelle ROM compatible avec votre appareil. Sachez néanmoins que la plupart des ROM Custom intègrent des fonctionnalités ou des applis qui nécessitent le root. Il serait dommage de passer à côté de ces avantages !



INFOS [**KINGO ROOT**] Où le trouver ? [www.kingoapp.com]

[**SUPERSU**] Où le trouver ? [<https://goo.gl/4lwbmP>]

[**ROOT CHECKER**] Où le trouver ? [<https://goo.gl/Lg1lb4>]

Difficulté : ☠☠☠

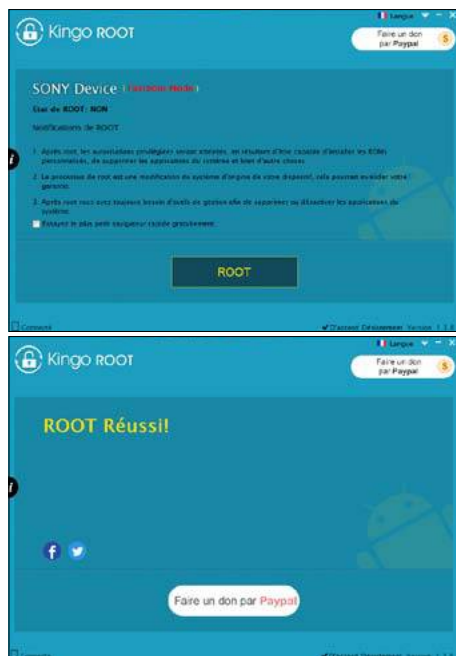
COMMENT FONCTIONNE KINGO ROOT ?

PRATIQUE



01 > AVEC UN PC

Sur le site, allez dans **Product** et téléchargez **Android Roor for Windows**. Téléchargez, installez et lancez le programme. Lorsqu'on vous le demandera, il faudra brancher votre appareil avec un câble USB et simplement cliquer sur le gros bouton **ROOT** (décochez la case au-dessus). Une fois les fichiers chargés, et si tout se passe bien, vous verrez **ROOT Réussi!**



02 > SANS PC

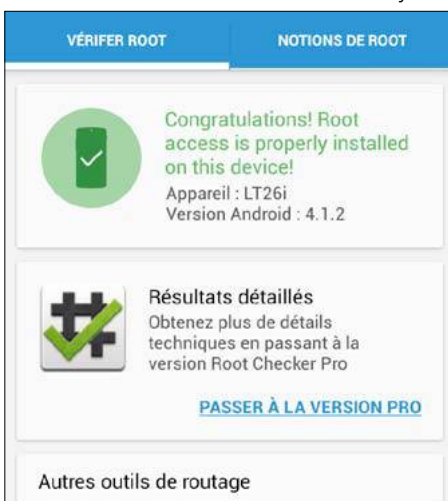
Toujours dans la partie **Product** du site, téléchargez **APK ROOT for Android** et installez-le sur votre mobile (en utilisant un explorateur de fichier). Lancez l'appli et attendez. Au bout de quelques minutes (n'éteignez pas votre téléphone!), un message affichera **ROOT**

SUCCEED. Quelle que soit la méthode utilisée, redémarrez votre appareil.



03 > VÉRIFIEZ QUE TOUT EST NORMAL

Téléchargez l'application Root Checker et choisissez **Vérifier l'accès root**. Si vous voyez





HACKING

Root & ROM Custom

un message vert c'est que tout est bon, votre téléphone est rooté! Si vous voyez un message orange, c'est que quelque chose s'est mal passé. Recommencez et redémarrez l'appareil avant de réessayer Root Checker. Encore raté? Tentez alors Towelroot ou Framaroot (voir encadré).

04 > INSTALLER SUPER SU

Super SU est une application indispensable pour les appareils rootés. Il s'agit en fait d'une protection contre des applis potentiellement dangereuses. En effet si certaines applis normales vous donnent des droits supplémentaires c'est aussi le cas des applis malsaines! En plus Super SU permet de «dé-rooter» temporairement ou définitivement votre appareil et de vérifier à tout moment quelles applis ont l'accès root.



DEUX AUTRES MÉTHODES

Kingo Root n'a pas fonctionné avec votre téléphone? Il existe deux autres méthodes ne nécessitant pas d'ordinateur. Towelroot et Framaroot sont des fichiers APK qui peuvent se lancer directement sur votre appareil Android. Pour le premier il suffira d'appuyer sur make it ra1n pour lancer le processus. Si l'appareil redémarre, c'est que cela n'a pas marché. Pour le second il faudra choisir entre les deux méthodes: Aragorn ou Gandalf. L'appli vous dira de suite si votre appareil est compatible... ou pas.





INFOS [**KINGO ROOT**] Où le trouver ? [www.kingoapp.com]

[**SUPERSU**] Où le trouver ? [<https://goo.gl/4lwbmP>]

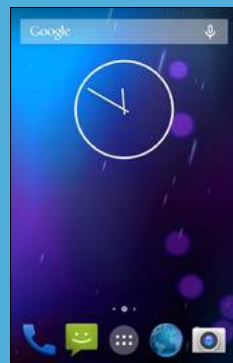
[**ROOT CHECKER**] Où le trouver ? [<https://goo.gl/Lg1lb4>]

Difficulté: ☠☠☠

➔ NOTRE SÉLECTION DE CUSTOM ROM

> CyanogenMod

CyanogenMod est la ROM Custom la plus populaire. Elle offre une compatibilité de très nombreux appareils avec une sélection d'applis intéressantes et des fonctionnalités liées à la sécurité (chiffrement, VPN, etc.) Il est possible de redémarrer son téléphone comme sous Windows ou de partager sa connexion de plusieurs manières. On compte aussi des améliorations de la gestion de la mémoire et du CPU par rapport aux versions d'Android sur lesquelles CyanogenMod est basée. Une version spéciale de cette ROM est disponible pour une installation plus facile et sans risque (voir notre pas à pas).



> Paranoid Android

C'est la ROM Custom qui fait parler d'elle en ce moment. Paranoid propose une interface graphique tablette/phablette adaptée aux petits écrans. L'accent est mis sur les notifications qui se veulent plus graphiques et interactives. Le mode Pie est une sorte de barre des tâches qui permet de passer très facilement d'une appli à une autre. Attention cette ROM est limitée à la gamme Nexus et à une trentaine d'autres terminaux.



> AOKP

AOKP (Android Open Kang Project) est une ROM Custom permettant de personnaliser les raccourcis présents dans les paramètres rapides (la deuxième partie de la barre d'états). En parallèle, cette ROM inclut aussi une fonctionnalité dénommée "Navigation ring", qui permet d'assigner des accès rapides à des applications de votre choix. Parmi les autres fonctionnalités un peu plus "gadgets" citons le contrôle des permissions, la personnalisation des vibrations ou des allumages LED et une fonction «overclock» native.





HACKING

Root & ROM Custom

CYANOGENMOD FACILE !

PRATIQUE



POUR EN PROFITER PLUS FACILEMENT DE CYANOGENMOD, LES DÉVELOPPEURS ONT LANCÉ UN «INSTALLER». IL S'AGIT EN FAIT D'UNE APPLICATION ANDROID ET D'UN PROGRAMME WINDOWS. EN QUELQUES ÉTAPES, ET SOUS RÉSERVE DE POSSÉDER UN APPAREIL COMPATIBLE, VOUS ALLER ROOTER VOTRE TÉLÉPHONE, DÉBLOQUER LE BOOTLOADER ET INSTALLER LE SYSTÈME EN UNE SEULE FOIS !

01 > L'APPLI

Pour avoir un aperçu des différentes étapes, il suffit d'aller sur le site de Cyanogen (www.cyanogenmod.org) et de faire **Get Start**. Il faudra en fait télécharger l'application pour votre smartphone ou tablette (<http://get.cm/app>) et l'installer. Il faudra juste auparavant s'assurer dans les **Paramètres** que vous avez autorisé l'installation des applis qui ne sont pas issues du Google Play Store.



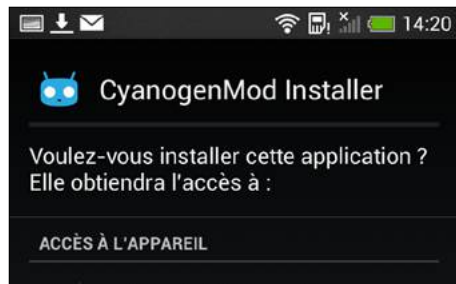
03 > LA CONNEXION

Le programme va premièrement vous demander de désactiver votre antivirus. Faites **Continue** pour qu'une fenêtre vous propose de connecter votre appareil au PC via le câble USB. Au bout de quelques secondes, votre smartphone sera reconnu (si votre appareil n'est pas compatible, le programme vous le dira à ce moment seulement). Faites **Install** et laissez faire le transfert de fichiers. Bien sûr, ne débranchez pas votre appareil!



02 > QUELQUES RÉGLAGES...

L'appli vous demandera ensuite d'activer le **Débogage USB** et de désactiver le **Fastboot** (**Démarrage rapide**). Pas la peine de chercher dans les menus, on vous proposera des raccourcis. Lorsque tout sera bon, l'appareil vous proposera de poursuivre les manipulations sur votre PC avec le programme Windows. Attention, si vous n'avez pas encore fait de sauvegarde de vos données, c'est votre dernière chance!



04 > CYANOGENMOD SUR VOTRE MOBILE!

Lors du redémarrage, vous verrez le logo Cyanogen sur votre téléphone. Sur PC, faites **Exit** lorsque le processus sera terminé. Peu de temps

après, votre nouvelle Custom ROM sera accessible dans sa version la plus récente. Il faudra tout reconfigurer, de la langue au réglage de l'heure en passant par votre compte Google. Notez que vous pouvez aussi vous inscrire pour avoir un compte Cyanogen (localisation de votre appareil et effacement à distance en cas de vol)...





INFOS [AIRDROID]

Où le trouver ? [<https://goo.gl/TkqJnE>]

Difficulté : 



-EN LOCAL / À DISTANCE- UN **ACCÈS** À VOTRE APPAREIL ANDROID

AirDroid est une application qui une fois installée sur votre appareil Android permet d'y avoir accès depuis un PC ou un Mac. Vous pourrez donc accéder à vos SMS et y répondre, transférer vos fichiers, écouter votre musique et accéder aux notifications. La connexion fonctionne à distance (en WiFi et 3G), mais aussi en local depuis le même réseau domestique.



HACKING

Contrôle à distance

Voici une appli qui va vous devenir indispensable si vous avez un appareil sous Android (et que vous ne l'utilisez pas uniquement pour téléphoner !). AirDroid va étroitement lier votre smartphone, tablette ou Media Center Android à votre ordinateur. L'interface est très bien conçue et permet à distance avec Internet ou en local avec votre réseau WiFi domestique d'accéder à vos fichiers et de les transférer (d'un côté comme dans l'autre), de répondre à un appel rentrant ou à un SMS, d'afficher vos contacts et vos notifications.

DES FONCTIONNALITÉS AVANCÉES

Parmi les fonctionnalités annexes, on compte aussi un désinstalleur d'application, un nettoyeur de RAM, un module de géolocalisation et

de partage de connexion. Avec un appareil rooté vous pouvez même virtualiser l'interface de votre appareil Android dans une fenêtre et naviguer dans votre téléphone ou votre tablette comme si vous l'aviez dans les mains. Sur PC ou Mac, il faudra juste installer le logiciel client, mais ce n'est même pas obligatoire puisqu'à l'origine AirDroid fonctionnait depuis un navigateur. Cette fonction est toujours présente on peut donc imaginer répondre à un coup de téléphone depuis n'importe quel appareil (si par exemple vous avez oublié votre téléphone à la maison). Et si vous pensez que tout cela doit être bien compliqué, vous allez être surpris !



Un contrôle total sur votre appareil Android sans avoir à le sortir de votre poche et un moyen très sympa de partager des fichiers



Le module AirMirror nécessite un téléphone rooté



PRENEZ LE CONTRÔLE DE VOS APPAREILS ANDROID À DISTANCE !

L'INTERFACE WEB

Pas besoin d'installer de client sur un ordinateur pour avoir accès à AirDroid. Si vous n'êtes pas chez vous ou si vous avez un ordinateur sous Linux vous pouvez utiliser l'interface Web en suivant notre lien. Il suffit d'entrer vos identifiants pour profiter de toutes les fonctionnalités de l'appli.

Lien : <http://goo.gl/1mXdlr>





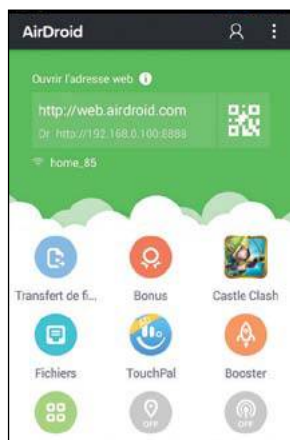
COMMENT FONCTIONNE AIRDROID ?

PRATIQUE



01 > SUR VOTRE TÉLÉPHONE

Installez l'appli sur votre appareil, ouvrez



un compte et activez les notifications. L'interface n'a rien de très complexe. Vous trouverez les fonctionnalités annexes (géolocalisation, booster de RAM, etc.) que nous vous laissons découvrir. Concentrons-nous maintenant sur le client.

02 > SUR VOTRE PC/MAC

Vous pouvez utiliser l'interface Web (voir notre encadré), mais le logiciel client est tout indiqué pour une utilisation à la maison. Suivez ce lien : <http://goo.gl/tB6V84>. Entrez les identifiants que vous vous êtes choisis auparavant et autorisez le programme à passer au travers de votre pare-feu. Bienvenue dans AirDroid! D'ici, vous pouvez ajouter des amis et envoyer des fichiers de toutes tailles.



AIRMIRROR, POUR LES APPAREILS ROOTÉS

Sur la gauche vous verrez une icône en forme de jumelles, il s'agit du AirMirror. Si vous avez un appareil rooté (voir page 6 et 12) vous y aurez accès. Dans une fenêtre vous pourrez voir l'intégralité de l'interface du téléphone. Il est possible de saisir le schéma de déblocage à la souris, de prendre des captures, d'ouvrir les applis, de prendre une photo, etc. Lorsque vous utilisez ce mode virtuel, les manipulations seront aussi visibles sur le téléphone. Nous avons même pu allumer la lampe torche et retoucher des photos !



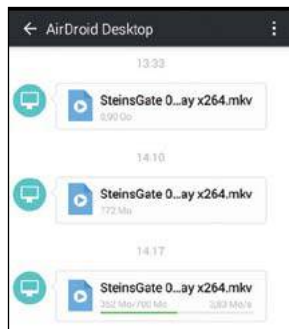


HACKING

Contrôle à distance

03 > TRANSFERTS ET NOTIFICATIONS

La première fonctionnalité que vous avez testée a été le transfert de fichier. Si vous voulez voir un film

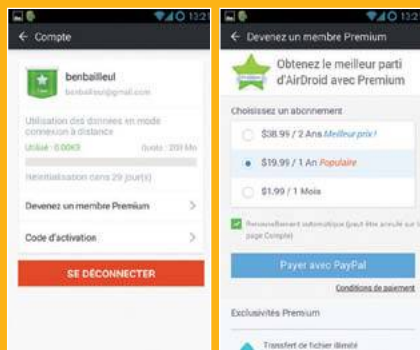


que vous avez téléchargé sur le PC, trouvez l'appareil cible (dans **Contact** ou **À proximité**) et faites un glisser-déposer dans la fenêtre. En 5 minutes, votre fichier atterrira dans votre appareil mobile.



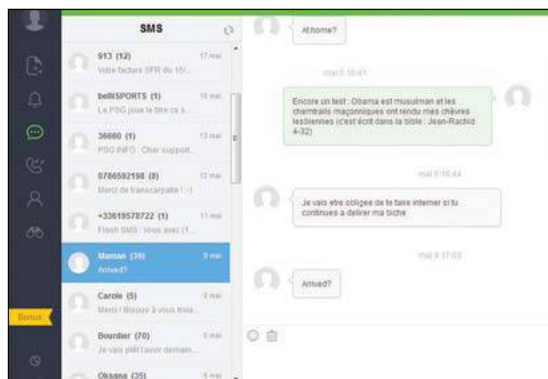
LA VERSION PREMIUM

AirDroid est gratuit, mais si vous utilisez plus de deux appareils (le client ne compte pas) ou si vous utilisez beaucoup le trafic à distance vous devrez passer par le mode **Premium**. Cela coûte 2 dollars/mois ou 20 dollars pour un an, mais il est possible d'accéder à une version **Bonus** (limité à 200 Mo de trafic) sans payer. Il suffit pour cela de faire la promotion de AirDroid auprès de vos amis.

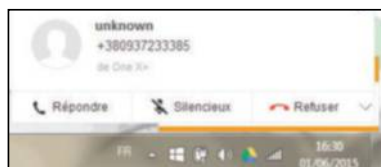


04 > SMS ET APPELS

Encore en dessous vous aurez la liste de vos notifications, de vos **SMS**, des appels entrants



et des contacts. Bien sûr vous pouvez interagir avec tout: répondez à un SMS sur le clavier de votre PC par exemple. Il n'est pas possible de déclencher un appel, mais on peut y répondre à condition d'avoir une paire d'enceintes et un micro.

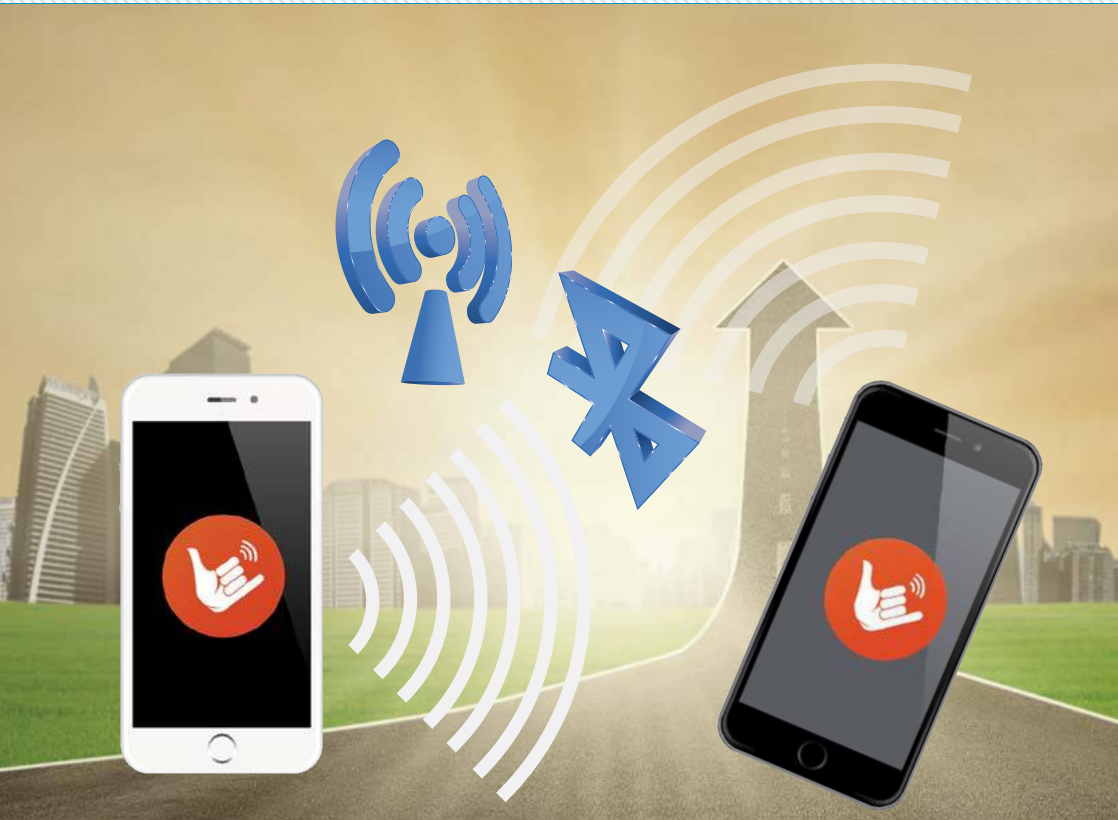




INFOS [FIRECHAT]

Où le trouver ? [<https://goo.gl/uHVx5j>]

Difficulté :  



COMMUNIQUEZ SANS RÉSEAU ET SANS INTERNET

VOUS PENSEZ QU'IL EST IMPOSSIBLE DE COMMUNIQUER DE TÉLÉPHONE À TÉLÉPHONE SANS AVOIR ACCÈS AU RÉSEAU GSM OU À INTERNET ? DÉTROMPEZ-VOUS ! MÊME SI LA PORTÉE EST LIMITÉE IL EST POSSIBLE D'UTILISER LE BLUETOOTH ET LE WiFi POUR ENVOYER MESSAGES ET PHOTOS À UN CORRESPONDANT.



Imaginez-vous à la montagne, dans un avion, à la plage ou en plein cœur d'un hiver atomique (appelé aussi «Cantal») : pas de réseaux GSM, pas de 3G et pas de connexion WiFi. Pourtant avec votre smartphone ou tablette équipés vous pouvez tout de même envoyer des messages et des photos à un correspondant se situant à 70 mètres maximum. Les deux appareils équipés de

l'application FireChat vont en effet communiquer ad hoc, sans points d'accès.

ALLUME LE «MESH» !

Si d'autres utilisateurs sont dans les parages, la portée est plus grande : il s'agit d'un «mesh» ou réseau maillé. Chaque intervenant peut recevoir, envoyer et relayer les données du réseau. La faiblesse de ce type de topologie réside dans la difficulté de trouver



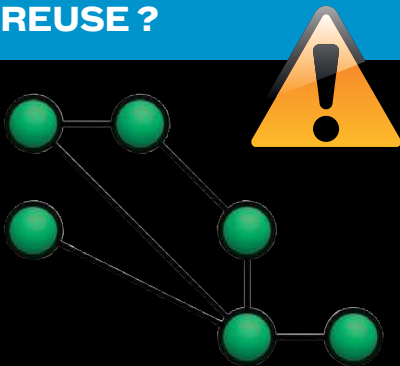
Une expérience sympa plus qu'un moyen de communication alternatif



Ne doit pas être utilisé pour des conversations sensibles

UNE APPLICATION DANGEREUSE ?

Pour éviter les malentendus, précisons que FireChat n'est pas une solution sûre pour échanger des messages. En effet, rien n'est chiffré dans le protocole et il est facile pour un gouvernement hostile de s'introduire dans les conversations. FireChat a été pointé du doigt lors des révoltes à Hong Kong en 2014. Privé de réseaux téléphoniques et 3G, les manifestants avaient alors utilisé l'appli pour communiquer et s'organiser. Même si Open Garden (la société éditrice) n'a jamais décrit FireChat comme une appli permettant d'anonymiser les conversations, elle a subi des critiques sur Internet à cause de la facilité avec laquelle certaines informations étaient interceptables. Les critiques ciblaient aussi la nécessité de se créer un compte. Cependant il n'y a pas de vérification d'e-mail dans le processus. Une personne peut donc mettre des informations complètement bidon et utiliser FireChat



Comme on peut le voir sur cette représentation graphique, un réseau en maillage (mesh) n'a pas besoin de serveur central. Chaque point vert représente un participant (ou pair) et plus il y a de monde, plus la portée du réseau est vaste.

sans problème. Le seul point noir, pour nous, reste les nombreuses autorisations superflues que demande l'appli : accès aux contacts, position précise, recherche des comptes, etc. Bref, FireChat n'a rien de dangereux à condition de ne pas l'utiliser pour des activités pour lesquelles l'appli n'a pas été conçue.



des pairs pour se connecter. Avec un ami, dans un village de 300 habitants vous ne pourrez communiquer qu'à 2 tandis que dans les endroits bondés des grandes villes vous aurez plus de chance de trouver des gens à qui parler. L'appli a du succès, mais pas assez pour remplacer les moyens traditionnels de communication. Les créateurs ont donc ajouté une option permettant aussi d'emprunter Internet lorsqu'il est disponible. Le résultat est forcément moins intéressant, mais efficace. FireChat se présente comme un client IRC avec

beaucoup de personnes connectées et la possibilité de rejoindre des «salons». En passant par Internet vous serez en priorité dirigée vers le pays dont provient votre IP. FireChat est donc une expérimentation sympa qui pourra vous être utile dans certaines occasions bien précises ou lors de certaines manifestations. On peut imaginer un groupe de musique essayer de faire le plus grand mesh possible le temps d'un concert en réunissant les fans dans un salon #concert ou un réseau éphémère qui serait créé le temps d'un néo-Woodstock (on a bien le droit de rêver !)



UNE APPLI QUI NE DOIT PAS ÊTRE UTILISÉE POUR DES CONVERSATIONS SENSIBLES

COMMENT FONCTIONNE FIRECHAT ?

PRATIQUE



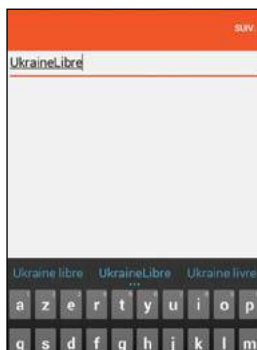
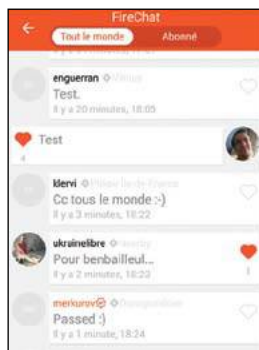
01 > PREMIERS PAS...

Pour vous inscrire, il faudra vous inscrire, mais l'appli ne vérifiera pas votre adresse e-mail. Mettez n'importe quoi si cela vous chante, vous pourrez utiliser FireChat de toute manière... Choisissez-vous un avatar et faites **Enregistrer**. Réalisez cette étape lorsque vous êtes connectés à Internet.



HACKING

Expérimentation

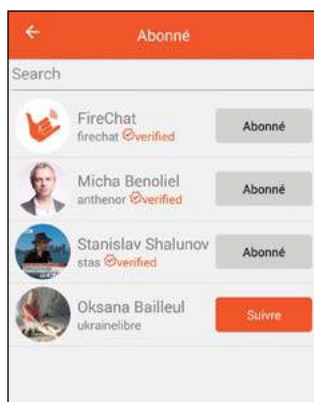
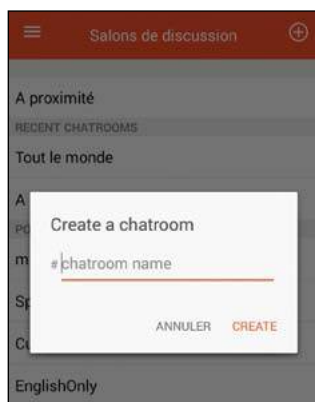


02 > À DISTANCE OU À PROXIMITÉ

Dès lors vous serez jeté dans la fosse aux lions avec des centaines de messages issus de différents endroits du globe: là où il se déroule quelque chose (comme le festival du film de Sundance au moment où nous écrivons ces lignes) et des utilisateurs de votre pays de connexion. En faisant **Découvrir** vous pourrez retrouver des utilisateurs à distance ou à proximité.

03 > TROUVEZ VOS AMIS

Dans les options (la flèche en haut à gauche), vous aurez à disposition les salons de discussions en vogue ou si vous désirez uniquement chercher des personnes dans votre zone, tentez le **#àproximité**. Si vous voulez vous retrouver entre amis, créez un salon et rameutez du monde en utilisant les réseaux sociaux (si Internet est disponible).

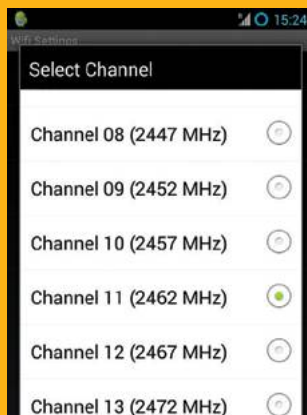


04 > DERNIER MOT

Il est aussi possible de **Suivre** vos amis pour vous retrouver plus facilement. Parfois la connexion sans Internet prendra un peu plus de temps à se mettre en place. Il faudra être patient. Attention, contrairement à ce qui est suggéré dans la vidéo de promo, l'appli ne fonctionne pas en mode avion et même aucun salon n'est privé.



SERVAL, UN PROJET AMBITIEUX



Il existe d'autres projets d'appli permettant de communiquer des messages textes via Bluetooth comme EnsiChat ou FireChat, mais tous sont plus ou moins isolés et proposent une portée assez réduite. A l'inverse nous avons découvert Serval Mesh. Malheureusement cantonné au système Android ce dernier est un projet mis en place en partenariat avec la croix rouge néo-zélandaise en cas de catastrophes naturelles et qui permet de communiquer par texte et par la voix ! Comme dans un réseau maillé, pas besoin de réseau centralisé pour faire fonctionner l'appli, il suffit de deux téléphones pour communiquer. Il est possible d'utiliser un réseau WiFi existant ou de faire office de point d'accès. Malheureusement le véritable mesh n'est disponible qu'avec les téléphones rootés. Le projet est Open Source et les concepteurs tentent de lever des fonds depuis quelques années pour améliorer le système et ajouter des antennes relais au réseau pour accroître sa portée. Cerise sur le gâteau vous pouvez télécharger l'appli depuis l'appareil de quelqu'un qui l'a déjà téléchargé. En cas de coup dur, vous pourrez donc faire partie du réseau. Un sacré projet dont nous vous parlerons prochainement plus en détail...

Lien : www.servalproject.org



**NUMÉRO
EXCEPTIONNEL**

TOP 570 APPLIS

LES MEILLEURES APPLIS GRATUITES

3,90€
seulement

Le **GUIDE
2015**
des
applications
ANDROID



CHEZ VOTRE MARCHAND DE JOURNAUX



INFOS [WiFi Map]

Où le trouver ? [<http://goo.gl/VJcu7F> (Android)] [<http://goo.gl/IMdcHs> (iOS)]

Difficulté : ☹️☹️☹️

TOUJOURS UN HOTSPOT SOUS LA MAIN

LORSQUE VOUS N'ÊTES PAS CHEZ VOUS, TROUVER UN POINT D'ACCÈS WiFi RELÈVE PARFOIS DE LA MISSION IMPOSSIBLE. BIEN SÛR VOUS POUVEZ COMPTER SUR VOTRE "FORFAIT DATA" (3G/4G) MAIS LE WiFi S'AVÈRE PLUS RAPIDE ET PLUS ÉCONOMIQUE. WiFi MAP VOUS PERMET DE VOUS CONNECTER GRATUITEMENT SUR DES HOTSPOTS ALENTOUR GRÂCE À SA COMMUNAUTÉ ALTRUISTE.



Si vous avez la bougeotte, vous aimeriez peut-être pouvoir éviter de défoncer votre forfait 3G/4G lorsque vous n'êtes pas chez vous. Il existe bien sûr les hotspots communautaires comme Free Wifi ou SFR FON, mais il n'est pas toujours aisé de trouver une box « amie » dans les parages... surtout

à l'étranger ! WiFi Map est une application mobile pour Android et iOS qui recense un grand nombre de points d'accès sur une carte interactive. Bien sûr, les mots de passe de ces derniers ont été partagés par d'autres utilisateurs. Vous pouvez même partager le mot de passe de votre propre réseau local... à vos risques et périls.



Une grosse communauté mondiale



Il faut parfois payer pour télécharger à l'avance des listes de mots de passe dans telle ou telle ville.



UNE CARTE INTERACTIVE
AVEC DES MILLIERS DE
HOTSPOTS DISPONIBLES



COMMENT FONCTIONNE WIFI MAP ?

PRATIQUE



01 > PARTAGEZ VOTRE RÉSEAU

Après le démarrage de l'appli, on vous demandera d'ajouter le réseau sans fil d'où vous vous connectez actuellement. Faites

Add si vous désirez le partager. Attention, s'il s'agit de votre réseau domestique vous n'êtes pas à l'abri d'un pirate.

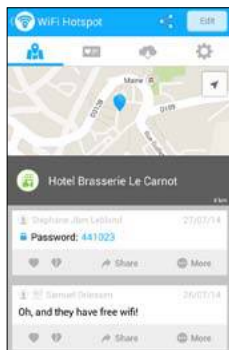
Dans le cas contraire (McDo, hôtel, bar, bibliothèque, etc.) rien ne vous empêche de partager le mot de passe. Entrez le mot de passe lorsque

l'appli vous le demandera. Ce duo SSID (nom du hotspot)/mot de passe ira dans la base de données de l'appli et les autres utilisateurs pourront en profiter.

02 > LE HOTSPOT LE PLUS PRÈS

Dans le cas où vous recherchez vous même un hotspot il suffit d'en choisir un dans la liste qui vous sera donnée en fonction de votre emplacement. Sélectionnez-en un pour avoir le nom et le sésame du hotspot le plus près de l'endroit où vous êtes. Si vous n'êtes pas connecté, il faudra obtenir la liste de mots de passe avec la 3G/4G mais si vous

n'avez pas de forfait data (ou pas de réseau) il faudra être prévoyant.



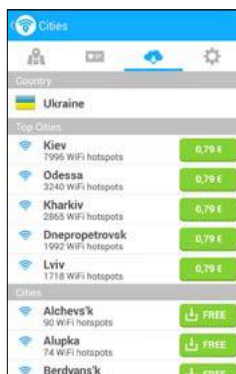
03 > TÉLÉCHARGEZ TOUS LES POINTS D'ACCÈS D'UNE VILLE

Car il est possible de télécharger à l'avance tous les hotspots connus par WiFi Map. Si vous savez que vous vous rendez dans une ville, allez dans l'onglet avec le petit nuage et faites une recherche parmi les pays et les villes. Dans notre exemple il existe 209 hotspots disponibles dans la ville du Havre et l'icône **Free** à côté montre qu'il est possible de les télécharger tous gratuitement. Il suffit pour cela d'ouvrir un compte.



04 > LA VERSION PRO

Pour certaines grandes villes ou des hotspots à l'étranger il faudra sans doute payer. Pour obtenir la liste des 7996 hotspots à Kiev en Ukraine, il faudra procéder à une microtransaction de 0,79 €. Vous pouvez payer par Paypal, avec une carte prépayée, un code ou en demandant une facturation sur le compte de votre fournisseur d'accès. Si vous voyagez beaucoup, libre à vous de choisir la version Pro de l'appli à 5 € pour profiter des listes de hotspots sans limitation..





UN PORTABLE À PLEINE PUISSANCE !

NOS CHERS SMARTPHONES ET TABLETTES SONT DE PLUS EN PLUS PUISSANTS ET EMBARQUENT TOUJOURS PLUS D'ÉLECTRONIQUE TRÈS AVANCÉE. SUR DES APPAREILS ROOTÉS (VOIR PAGE 8 ET 14) IL EST POSSIBLE D'OVERCLOCKER LE PROCESSEUR POUR AMÉLIORER LES PERFORMANCES, MAIS AUSSI DE FAIRE L'INVERSE POUR ÉCONOMISER DE LA BATTERIE...



Simple, aucun risque de casse et paramétrable à souhait



Ne permet pas un overclock à la manière de ce qui est pratiqué sur PC

L'overclock (ou «surcadencement» en français) permet de faire fonctionner un processeur au-delà de ses limites. Si votre jeu préféré rame un peu ou si votre interface Android se traîne un peu, il est possible d'y remédier. À l'opposé si votre problème se situe au niveau de l'autonomie, vous pouvez très bien commander à votre téléphone de ne fonctionner qu'au tiers de ses capacités. Dans la réalité, votre processeur (CPU) ne fonctionne

pas à 100 % tout le temps. Il oscillera entre 20 et 100 % en fonction de ce que vous lui demandez : jeux, navigation internet, veille, etc. No-Frills CPU Control fonctionne de manière intelligente puisqu'il propose plusieurs profils à paramétrer avec une plage de cadencement à régler vous-même. Vous ne pourrez pas utiliser votre CPU à 120 %, mais vous pourrez lui dire de fonctionner tout le temps à 100 % puis changer d'avis lorsque la batterie crierait famine...



LE CHOIX DE LA PUISSANCE AVEC NO-FRILLS CPU CONTROL

PRATIQUE


01 > L'INTERFACE

L'interface est très claire et en français.

Réglez les fréquences **maximale** et **minimale** puis choisissez un profil. Mettez tout au max pour les



jeux dans le profil (**Gouverneur**) **performance** et tout à 50% dans **powersave**. Vous n'aurez ensuite qu'à choisir le profil en fonction de l'utilisation.

Gestionnaire E/S concerne la gestion des données: **noop** permet d'économiser la durée de vie de la mémoire flash, **cfq** tente de distribuer équitablement la RAM entre les processus et **deadline** impose une coupure au process pour prévenir un manque de ressource.

02 > LES STATISTIQUES

Pour savoir quand votre processeur travaille et à quelle cadence, faites un tour dans les **Stats de fréquences** (les trois traits horizontaux en haut à droite). Vous verrez la fréquence actuelle ainsi que celles utilisées les 5 dernières minutes: pratique pour savoir quelle appli utilise quelles ressources.

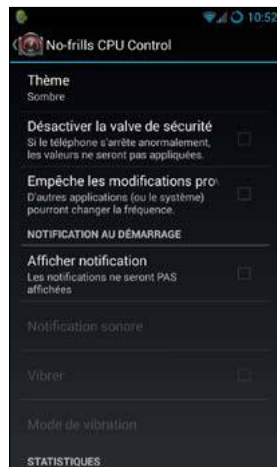
Fréquence	Total	Dernières 5 s
Fréquence actuelle: 1,7 GHz		
1,7 GHz	14,99 %	0,00 %
1,7 GHz	1,27 %	0,00 %
1,7 GHz	1,19 %	0,00 %
1,7 GHz	16,59 %	0,00 %
1,7 GHz	40,39 %	0,00 %
1,7 GHz	2,58 %	0,00 %
1,7 GHz	2,81 %	0,00 %
1,7 GHz	13,84 %	0,00 %
1,7 GHz	0,74 %	0,00 %
1,7 GHz	0,16 %	0,00 %
1,7 GHz	0,12 %	0,00 %
1,7 GHz	0,19 %	0,00 %
1,7 GHz	1,48 %	0,00 %

03 > LES PARAMÈTRES

Dans les **Paramètres** (les trois petits

points), il est possible d'ajouter une sécurité.

En effet un processeur qui fonctionne à 100% tout le temps va chauffer. Si votre téléphone s'arrête de manière inopinée, les réglages d'overclocking seront annulés. En cochant la deuxième case, vous autorisez le système à faire des corrections sur vos réglages.



ET SUR IPHONE/IPAD ?

Comme vous pouvez l'imaginer, il n'existe pas d'appli de ce type sur iPhone/iPad à moins d'avoir un appareil jailbreaké (voir page 10 et 12). Pour les petits bidouilleurs, vous pouvez toujours tenter iOverclock que vous trouverez sur le marché alternatif Cydia.





INFOS [DSPLOIT] Où le trouver ? [<http://goo.gl/WTFbSa>]

[BUSYBOX] Où le trouver ? [<http://goo.gl/hMLMve>]

Difficulté :

TESTEZ & SÉCURISEZ VOTRE RÉSEAU

VOUS VOULEZ VÉRIFIER LA SÉCURITÉ DU RÉSEAU Wi-Fi D'UN AMI ? PAS BESOIN DE VOUS DÉPLACER AVEC UN PC SOUS KALI PUISQU'AVEC UN MOBILE SOUS ANDROID ET L'APPLI DSPLOIT VOUS POURREZ LANCER TOUTE UNE BATTERIE DE TESTS : SNIF-FING, SIDEJACKING, CRACK DE MOT DE PASSE, ETC.



Couvre différents aspects de la sécurité en plus de ses fonctionnalités sympathiques



L'application est moins puissante que Kali Linux et nécessite un appareil rooté





Pour vérifier si votre réseau Wi-Fi et votre environnement informatique sont sécurisés de manière correcte, il existe plusieurs outils sous Windows ou Linux, mais lorsqu'il s'agit d'appareil mobile, les choix sont plus restreints. Les logiciels de ce type demandent, en effet, beaucoup de ressources et un téléphone, même puissant, ne pourra pas rivaliser avec un Intel Core i7. Pourtant, il existe des outils qui permettent de faire de vraies prouesses. dSploit est une application fonctionnant avec n'importe quel appareil rooté. Cette dernière permet de rechercher

dans votre réseau les vulnérabilités matérielles et logicielles connues, de scanner les ports, de sniffer des mots de passe, de manipuler le trafic et de réaliser des attaques de type «man-in-the-middle». Une fois dans un réseau privé ou public, vous avez accès à tous les périphériques et êtes libre de scruter ses moindres faiblesses...



UNE SUITE D'OUTILS
LÉGÈRE POUR
ANALYSER LES RÉSEAUX
ENVIRONNANTS

LES APPAREILS DE CHEZ PWNIE EXPRESS

Pwnie Express propose du matériel pour tester les réseaux sans fil. Parmi ces derniers, le Pwn Phone et le Pwn Pad sont équipés d'une distribution Linux spécialisée dans l'audit réseau (AirCrack-ng, Kismet, SQLNinja, Metasploit, etc.) et d'une clé Wi-Fi TP-Link autorisant l'injection de paquet. Les machines ne sont pas données, mais il est possible de télécharger gratuitement le logiciel pour le placer soi-même sur son appareil. Attention, seule la gamme Nexus est pour l'instant éligible.

Lien : www.pwnieexpress.com





INFOS [DSPLOIT] Où le trouver ? [<http://goo.gl/WTFbSa>]

[BUSYBOX] Où le trouver ? [<http://goo.gl/hMLMve>]

Difficulté :

À L'ASSAUT DE DSPLOIT !

PRATIQUE



01 > INSTALLATION

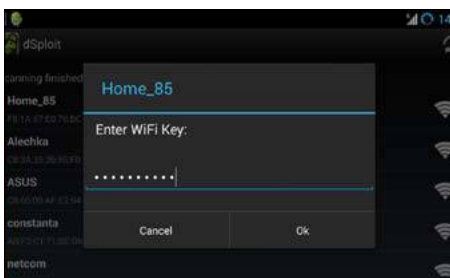
dSploit n'est pas disponible sur le Google Play Store, il faudra télécharger le fichier APK en suivant notre lien puis le transférer via le câble



USB ou vous l'envoyer par mail. Pour pouvoir l'installer, il faudra autoriser les sources inconnues. Allez dans **Paramètres > Sécurité** et cochez **Sources inconnues**.

02 > BUSYBOX ET MAPPAGE DU RÉSEAU

Telle quelle, l'application refusera de fonctionner, il faudra que vous installiez BusyBox. Pour cette dernière, pas de problème! Elle est disponible sur le Play Store. Lorsque vous la démarrerez,



faites juste **Install** en bas et attendez la fin du processus. Retournez dans dSploit et tout devrait fonctionner. Après quelques secondes de paramétrage, vous verrez tous les périphériques qui sont connectés à votre réseau local (il faut bien sûr que votre appareil Android en fasse partie).

ARP POISONING ?

En plus d'empêcher la connexion d'un appareil sur le réseau (depuis le menu MITM), l'ARP Poisoning permet de faire des petites blagues comme de remplacer toutes les photos ou vidéos d'un site par celle de votre choix.



marc, avril 25, 2015

Match retour chez Loria!



Enfin... "l'archeuse retour" photo

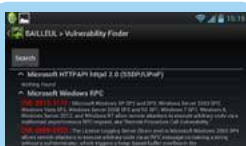




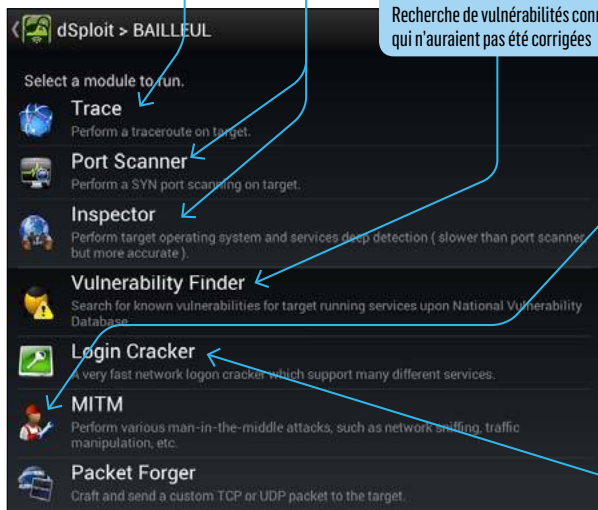
03 > LES FONCTIONNALITÉS

Traceroute permettant de suivre les paquets d'informations sur le réseau

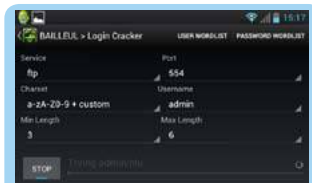
Scan de port standard et poussé



Recherche de vulnérabilités connues qui n'auraient pas été corrigées



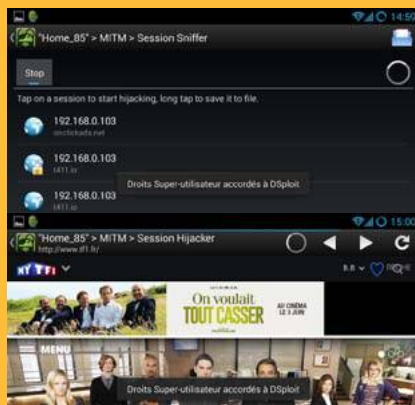
Attaques Man-in-the-Middle : sniffer de mot de passe, ARP poisoning (couper le Wi-Fi sur un périphérique, sidejacking, injection de script, remplacer des images, des vidéos, etc.)



Un petit logiciel de crack «brute force» pas très puissant mais pouvant se révéler utile

SIDE JACKING ?

Le sidejacking, ou «session hikacking» permet de voler l'accès à un site protégé par mot de passe. Vous ne crackez pas le mot de passe, mais vous vous invitez sur une session ouverte sur le réseau. Cette technique est le meilleur moyen pour savoir si le site en question dispose d'un vrai chiffrement SSL (le fameux «s» du «https»). Sur notre capture nous pouvons voir que le site de TFI ne dispose pas de cette protection et qu'il a été très facile de s'inviter sur le profil d'un utilisateur connecté au même réseau que nous.





TÉLÉCHARGER LES APPLIS DU GOOGLE PLAY STORE



// AVEC APK DOWNLOADER

Les utilisateurs d'appareils Android savent qu'il suffit de se connecter au Google Play Store depuis son PC pour pouvoir télécharger ses applis directement sur son téléphone. Il n'est pas possible de télécharger le fichier APK correspondant à l'application. Mais pour différentes raisons, vous pourriez avoir envie de garder une trace de ces fameux APK: appli qui pourrait disparaître du Store, un appareil Android non relié à Internet ou cassé, etc. Pour vous, il existe une solution, le site APK Downloader permet de récupérer un lien valide vers l'APK de votre choix en mettant l'URL de l'appli dans le champ. Il suffit ensuite de cliquer sur le lien en vert pour obtenir le fichier.



<http://apps.evozi.com/apk-downloader>

MONITORER LE SYSTÈME

// AVEC ANDROID TUNER

Avoir l'œil sur le moindre paramètre de votre smartphone et pouvoir les manipuler à votre guise, c'est l'utilité d'Android Tuner (disponible en version d'essai). Overclocking, tweaks divers, gel d'applications, sauvegarde, désinstallateur, explorateur de fichiers... Tout est là ou presque, surtout pour les appareils rootés.



<http://goo.gl/MzU8UU>



UNE CARTE SIM À LA BONNE TAILLE !



// AVEC iCLARIFIED

Vous changez de téléphone, mais voilà, votre vieille carte SIM est trop grande pour rentrer dans votre nouvel appareil. C'est parce qu'il s'agit d'un nouveau format: Micro ou NanoSIM en fonction du modèle. Au lieu de demander une nouvelle SIM compatible à votre opérateur



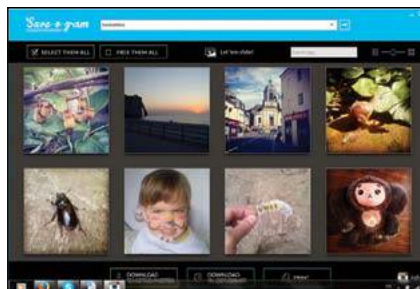
téléphonique, il existe une solution toute simple: couper votre carte SIM avec une paire de ciseaux! Suivez notre lien, téléchargez et imprimez le document à l'échelle d'origine. Placez votre carte SIM sur le modèle et à l'aide d'une règle et d'un crayon, tracez les lignes de découpe. Le rédacteur en chef a essayé cette technique pour vous avec son nouvel HTC et cela a parfaitement fonctionné pour lui! Si votre main tremble, laissez-vous une petite marge et tentez de rentrer la carte dans son nouvel emplacement. Allez-y par étapes successives. Bien sûr, veillez à sauvegarder les données stockées sur votre carte.



<http://goo.gl/OweUit>



RÉCUPÉRER SES PHOTOS INSTAGRAM



// AVEC **SAVE-O-GRAM**

Vous voudriez récupérer les photos stockées sur Instagram, mais l'appli ne dispose pas de cette fonctionnalité. Pas de problème avec Save-O-Gram, un logiciel PC qui va vous permettre de les télécharger directement depuis votre compte. Il suffit de taper votre pseudo en haut, de cocher les clichés que vous désirez (ou de faire **Select Them All**) puis de cliquer sur **Download in .ZIP Format**. Attention, votre compte devra être public pour que cela fonctionne. Si ce n'est pas le cas, il faudra le paramétrer en tant que tel sur votre appli Instagram le temps du téléchargement puis rebasculer le compte en privé à la fin du processus.

D'ailleurs, sachez que si votre compte est public, n'importe qui peut vous voler vos photos avec Save-O-Gram...

    <http://save-o-gram.com>

ENREGISTRER VOS MESSAGES SNAPCHAT



// AVEC **SNAPHACK**

Peut-être faites-vous partie des millions d'utilisateurs du logiciel Snapchat. Il s'agit d'une application permettant d'envoyer des messages, des photos ou de courtes vidéos qui s'autodétruisent au bout d'un temps déterminé par l'expéditeur. Cela permet notamment d'envoyer des messages sans laisser de traces. Si vous utilisez le mode capture d'écran, l'expéditeur sera mis au courant par le logiciel (donc si vous faites le malin, terminé les «sextos»), mais saviez-vous qu'il est tout de même possible de sauvegarder ces messages sans éveiller les soupçons? La solution s'appelle SnapHack!



    <http://goo.gl/gORR8Z>

ANALYSEZ VOTRE RÉSEAU



// AVEC **NETALYZR**

Si vous avez un appareil sous Android et que vous voulez tester votre réseau et les éventuels blocages de votre FAI, voici Netalyzr. Il s'agit d'une application développée par



des chercheurs de l'université de Berkeley qui va scanner votre environnement à la recherche de précieuses données : problème TCP, compatibilité UPnP, performance, temps de latence, présence de proxys, test DNS, support de l'IPv6, détection du NAT, etc. Idéal pour voir si votre fournisseur bride certains protocoles ou utilise des procédés contre la neutralité du Net. Attention, le vocabulaire est très pointu. L'application fonctionne avec un appareil normal, mais si le vôtre est rooté, vous pourrez analyser plus en profondeur les méandres de votre connexion...

    <http://goo.gl/dKruWW>



PARTAGEZ VOS CLÉS WI-FI

// AVEC INSTABRIDGE



C'est le genre de situation que nous avons vécu au moins une fois : invité dans une soirée, vous

aimeriez bien vous connecter au réseau Wi-Fi de votre hôte, mais voilà, ce dernier n'est pas sûr de son code, l'a recopié sur un papier introuvable ou est occupé à raconter ses meilleures histoires de Toto. À l'opposé, vous êtes chez vous avec quelques amis et tous vous demandent tour à tour votre clé d'authentification. Pénible. La solution vient d'InstaBridge. Il suffit de l'installer et de choisir parmi votre liste de contacts ceux avec qui vous voulez partager votre réseau. Ils peuvent alors accéder à votre Wi-Fi sans entrer aucun mot de passe et sans même le connaître. Vous changez de mot de passe ? Cela ne change rien pour vos camarades tant que vous ne les supprimez pas de la liste de partage. Plus fort, il est possible de partager des réseaux Wi-Fi de cafés de McDo, etc. Si vos amis partagent leur réseau avec vous, et que leurs contacts ont aussi partagé leur réseau, vous avez donc accès au Wi-Fi des amis de vos amis !



www.instabridge.com

CONTOURNER LA VÉRIFICATION DE LICENCE

// AVEC LUCKY PATCHER



Lucky Patcher va simplement contourner la vérification des licences sur votre machine Android pour lancer les applis que vous avez déjà achetées (ou que vous ne voulez pas payer tout de suite). Téléchargez et installez Lucky Patcher sur votre appareil rooté (avec la BusyBox d'installée). Installez l'APK de l'application

que vous convoitez, mais surtout ne la démarrez pas. Utilisez le mode Auto et attendez que Lucky Patcher aille chercher le patch adéquat. Selon l'appli, il vous sera peut-être demandé de copier à la main les dossiers d'une licence dans `/sdcard/Android/Obb`. Lucky Patcher ne fonctionne pas avec votre fichier APK ? Pas de panique, les développeurs ajoutent des patches tous les jours !



<http://lucky-patcher.netbew.com>

BOOTEZ UN ISO DEPUIS SON SMARTPHONE

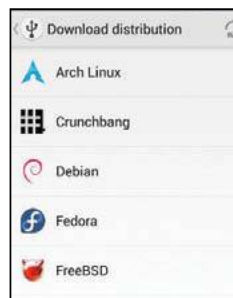
// AVEC DRIVEDROID



Si vous êtes du genre à booter votre PC sur des images ISO (une distribution Linux «Live CD» par exemple), cette petite appli Android va devenir indispensable. Au lieu de booter depuis le lecteur DVD ou une clé USB, vous pourrez stocker vos ISO sur votre téléphone ou tablette pour ensuite les utiliser avec votre ordinateur. À vous de relier votre appareil via le câble USB et de régler votre BIOS pour booter sur ce port (généralement F12 pour le «boot menu» ou F1 pour le «startup menu»). Vous ne serez jamais au dépourvu si vous voulez lancer BackTrack depuis le PC d'un copain...



<http://goo.gl/1XNR8>





BLOQUEZ APPELS ET SMS

// AVEC **TRUECALLER**

Entre les hotlines, les standards de publicité, ou même les serveurs automatiques qui vous informent que vous venez de gagner 15 millions d'euros, vous pouvez rapidement voir votre smartphone devenir une véritable centrale d'appels indésirables. La solution, vous la connaissez: mettre les numéros dans votre liste noire. Mais selon votre appareil et la version d'Android que vous utilisez, cela peut vite devenir un véritable parcours du combattant. Heureusement, des applications comme TrueCaller sont là pour vous simplifier la tâche. Que leur numéro soit affiché, ou non, en quelques secondes les correspondants indésirables sont ajoutés à votre «blacklist» et tomberont directement sur votre répondeur s'ils tentent de vous joindre. Vous pouvez même choisir de bloquer les SMS en plus des appels.



   <https://goo.gl/Spl0ch>
<https://goo.gl/YblSzJ>

DÉBARRASSEZ-VOUS DES PUBLICITÉS

// AVEC **ADBLOCK PLUS**



Célèbre sur navigateur PC, Adblock Plus bloque les publicités envahissantes et débarque sur Android. Pour l'installer il suffira d'autoriser l'installation d'applis «inconnues» (**Paramètres > Sécurité > Sources inconnues**). À l'ouverture, Adblock Plus va automatiquement chercher un «filtre» en fonction de votre pays



de résidence. Il s'agit d'une liste d'adresses Web que l'application va bloquer, puisque ce sont elles qui permettent aux applis d'afficher des publicités. Cette liste est régulièrement mise à jour pour ajouter d'autres adresses. Si vous voulez supprimer les pubs sur le navigateur, il faudra configurer votre proxy.

   <https://adblockplus.org/en/android-install>

FLASHEZ À VOLONTÉ

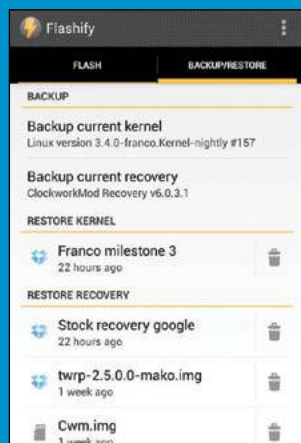
// AVEC **FLASHIFY**



Flasher une ROM peut parfois s'avérer pénible quand celle qui vous intéresse utilise une application dédiée pour l'installation. Flashify simplifie l'opération en permettant de flasher depuis votre smartphone, votre Dropbox ou votre explorateur de fichiers préféré. Dans sa version gratuite, vous pouvez installer trois ROMs par jour maximum.



<http://goo.gl/whA6co>



PROTECTION

41

DOSSIER ANTIVOL :
que faire pour se protéger ?

48

BOXCRYPTOR : un cloud chiffré

52

AVAST ! SECURELINE :
un VPN efficace

54

Un mot de passe principal
avec **DASHLANE**

56

SECRECY : votre coffre fort à fichier

58

IMSI CATCHER : êtes-vous surveillés ?

60

Empêchez les applis d'accéder à votre
compte Google+

62

ORBOT, le Tor version Android !

65

MOUCHARDS sur mobile : comment
ça marche et comment s'en
débarrasser ?

70

Faites le ménage avec **CCLEANER**

72

Restaurez vos applis avec **APPS
BACKUP & RESTORE**

74

Verrouillez l'accès à vos applis avec
APPLOCK

76

SMSSECURE : Chiffrez vos SMS





PROTECTION

Vol ou perte de smartphone

PERTE, VOL : QUE FAIRE POUR SE PROTÉGER ?

TABLETTES ET SMARTPHONES NOUS ACCOMPAGNENT PARTOUT, TOUT LE TEMPS. ILS CONTIENNENT TOUTES NOS INFORMATIONS PERSONNELLES (E-MAIL, CONTACTS, SMS, PHOTOS, ETC.) ET LES PERDRE OU SE LES FAIRE VOLER TIENT SOUVENT DU CATACLYSME. POUR ÉVITER LE DRAME, VOUS DEVEZ PRENDRE LES DEVANTS ET INSTALLER DES SYSTÈMES DE SÉCURITÉ. CAR MÊME SI VOUS PERDEZ VOTRE APPAREIL, VOUS POURREZ AU MOINS SAUVEGARDER VOS DONNÉES, LES EFFACER À DISTANCE ET MÊME VERROUILLER L'ACCÈS...





Tuez votre téléphone à distance ! Si vous vous faites voler votre bébé ou que vous le perdez sans espoir de le retrouver, il vous reste toujours une solution. Le rendre inutilisable. Plusieurs raisons à cela. D'abord, votre appareil peut contenir des photos privées, des numéros de téléphone importants, des informations bancaires, etc. Autant de données sensibles que vous ne souhaitez pas voir tomber entre n'importe quelles mains. Un vol de smartphone peut aussi, dans le pire des cas, rimer avec vol d'identité. Il stocke tellement

d'informations sur vous, que les voleurs les exploitent à des fins criminelles. Enfin, si vous perdez votre téléphone ou votre tablette, de manière plus égoïste, vous n'avez pas envie d'en faire profiter quelqu'un d'autre, encore moins un voleur.

APPLE EN AVANCE SUR GOOGLE...

Pour cela il existe la fonction Localiser mon iPhone (Find my phone ou Activation Lock) sur les appareils équipés d'iOS (voir encadré), mais sur Android c'est moins simple à cause du caractère «ouvert» du système. En effet il est facile pour un voleur de remettre à zéro votre téléphone en utilisant la réinitialisation usine. Avec un téléphone rooté et une appli comme Avast Anti-Theft, il est possible de signer votre SIM : impossible pour un voleur de faire



SUR IPHONE OU ANDROID, LES SOLUTIONS NE MANQUENT PAS POUR ÉVITER LES VOLS

KILL SWITCH : QU'EST CE QUE C'EST VRAIMENT ?

L'anglicisme Kill Switch (littéralement interrupteur pour tuer) désigne une fonctionnalité qui permet de verrouiller et de rendre inutilisable votre appareil à distance. Des variantes permettent également d'effacer le contenu de votre appareil. Ici, le précurseur c'est Apple. Lors de la présentation d'iOS 7 en 2013, le fabricant californien a intronisé cette fonctionnalité en grande pompe. Elle garantissait à l'époque de rendre un iPhone ou une tablette inutilisable, à distance. Selon les premiers retours, et d'après les témoignages de l'avocat général de New York, Eric Schneiderman, la fonction Kill Switch sur les iPhones fonctionne. Les vols d'iPhones auraient été réduits de 29 % à New York, de 38 % à San Francisco et de 24 % à Londres.





PROTECTION

Vol ou perte de smartphone



Sur iPhone, impossible d'accéder au contenu de l'appareil sans la saisie des identifiants. Certes le système est plus rigide, mais les voleurs sont démunis

fonctionner votre téléphone avec une autre carte. Pour les appareils non-rootés, cela devient compliqué. Il est en effet assez facile pour des voleurs organisés de contourner les limitations. Il suffit de faire une réinitialisation d'usine, en ayant pris soin, précédemment d'avoir désactivé le Wi-Fi et les données réseau. Ainsi le téléphone n'aura aucun moyen de communiquer avec vous à distance et, de plus, s'il est

réinitialisé, il n'y aura plus aucune trace de vous.

LES SOLUTIONS PRÉSENTES ET À VENIR

Depuis la dernière version Lollipop (5.1) le système Android intègre le Device Protection qui permet de protéger votre appareil contre le vol même avec un retour aux réglages d'usine. Le problème c'est que les mises à jour peuvent être longues à voir le jour et que si votre appareil est top vieux, vous n'aurez jamais accès à cette fonctionnalité. La solution ? Utiliser une application tierce comme Lookout (voir pages suivantes). Ici aussi un expert pourra utiliser le Recovery Mode pour tenter de bidouiller la ROM, mais tous les voleurs n'ont pas accès à ce niveau de technicité. Le risque zéro n'existe donc pas... pour l'instant.

la solution dédiée Avast Anti-Theft va encore plus loin avec les appareils «rootés». La signature de carte SIM est très efficace et fonctionne même en cas de réinitialisation !





QUELLE SOLUTION ANTIVOL CHOISIR ?

LES PRINCIPAUX DÉVELOPPEURS D'APPLI DE SÉCURITÉ SE SONT MIS À INTÉGRER DES FONCTIONNALITÉS ANTIVOL. VOUS POURREZ DONC PROFITER DE CERTAINES FONCTIONNALITÉS GRATUITES POUR RÉCUPÉRER VOS DONNÉES OU ÊTRE ALERTÉ EN CAS DE VOL... TOUR D'HORIZON.

	McAfee	Avast! Anti-Theft	Lookout	Norton	Bitdefender Anti-Theft
					
Site de gestion	www.mcafee-mobilesecurity.com	my.avast.com	www.lookout.com/fr	mobilesecurity.norton.com	my.bitdefender.com
Sauvegarde des données	oui	oui	oui	oui	non
Localisation	oui	oui	oui	oui	oui
Alarme	oui	oui paramétrable	oui	oui	oui
Verrouillage	oui	oui	oui	oui	oui
Suppression données	oui	oui	oui	oui	oui
Gratuit ?	oui	oui, existe en premium pour prendre en photo le voleur	oui pour la géolocalisation non pour les alertes antivol	non (évaluation gratuite 30jours)	non (évaluation gratuite 30jours)
Le plus	ergonomie intuitive	paramètres supplémentaires pour les appareils rootés comme activer le gps à distance	le voleur est pris en photo	blocage par sms	appli autonome
Le moins	paramétrages limités	complexe à paramétrer	principales fonctions dans la version premium	solution sécurité complète, mais lourde	besoin de l'accès administrateur
Note	★★★★☆	★★★★★	★★★★☆	★★★★☆	★★★★☆



PERTE OU VOL, GOOGLE EST VOTRE AMI

PRATIQUE



PAR DÉFAUT, VOTRE APPAREIL ANDROID DISPOSE DE FONCTIONNALITÉS POUR SAUVEGARDER ET RÉCUPÉRER VOS DONNÉES. MÊME SI ELLES SONT INEFFICACES EN CAS D'UNE RÉINITIALISATION USINE, POURQUOI NE PAS TENTER ? GOOGLE A ÉTÉ PLUS LOIN EN CRÉANT UNE FONCTIONNALITÉ À ACTIVER QUI PERMET DE LOCALISER, VERROUILLER ET EFFACER VOS DONNÉES À DISTANCE...

01 > LES PARAMÈTRES

Si vous n'avez pas coché l'option lors du démarrage, vous devrez vous rendre dans les

Paramètres de votre appareil et aller dans la partie **Sauvegarder et réinitialiser**. Cochez **Sauvegarder mes données** et **Restaurer automatiquement**.

Vérifiez bien que le compte associé à cette sauvegarde est le bon en appuyant sur

Compte de sauvegarde. Vous pouvez aller plus loin dans la sauvegarde automatique en acceptant d'envoyer vos documents dans le Cloud et en les synchronisant avec votre appareil.

02 > SAUVEGARDE ET LOCALISATION

Ainsi, si vous changez après une perte ou un vol, il vous suffira d'entrer votre adresse mail

pour récupérer vos données (agenda, contacts, e-mails, photos, films, etc.)

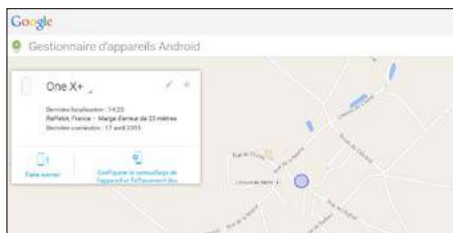
Pour cela, allez dans la section **Comptes des Paramètres** et sélectionnez le **Compte de sauvegarde**. Cochez

ensuite les données à sauvegarder. En cas de vol ou de perte, sachez que Google a prévu un outil pour localiser votre appareil et, le cas échéant, en effacer les données et le bloquer. Rendez-vous sur le site <https://www.google.com/android/devicemanager?hl=fr>.



03 > VERROUILLAGE À DISTANCE

Un menu déroulant vous permet de voir vos différents appareils enregistrés. Appuyez sur le bouton **Verrouiller** pour bloquer votre appareil à distance. Notez que vous devrez définir un nouveau mot de passe pour pouvoir le débloquer si vous remettez la main dessus. Notez que pour que cette fonctionnalité soit effective, vous devrez au préalable avoir autorisé l'application **Gestionnaire d'appareils** à verrouiller votre appareil à distance.



04 > EFFACER LES DONNÉES

Pour cela, allez dans les **Paramètres de sécurité** puis **Administrateurs de l'appareil** et vérifiez que l'appli est cochée. Sachez enfin

que vous pouvez aussi **Effacer vos données**. Toutes les applications, vos contenus multimédias et vos données personnelles seront effacés. Si votre appareil volé est

hors connexion, ceci ne fonctionnera que s'il est un jour à nouveau mis en ligne... patience donc.





INFOS [LOOKOUT] Difficulté : 

Où le trouver ? [<http://goo.gl/RNER8Z> (Android)]

Où le trouver ? [<http://goo.gl/1Q9hDD> (iOS)]

VOL ou PERTE DE SMARTPHONE : LA SOLUTION LOOKOUT



LA PLUPART DES APPLICATIONS DE SÉCURITÉ PROPOSENT UNE FONCTIONNALITÉ DE LOCALISATION. NOUS AVONS DÉCIDÉ DE LA TESTER AVEC LOOKOUT, L'ANTIVIRUS «HISTORIQUE» SUR ANDROID DISPONIBLE AUSSI SUR IPHONE ET IPAD.



Pas besoin de payer pour les fonctionnalités basiques



Le verrouillage à distance est payant, mais fonctionnel

« Je ne sais plus où je l'ai mis... et il est sous silencieux. »

Non, ce n'est pas Alzheimer qui vous guette, tout le monde a oublié son smartphone au moins une fois. Dans la voiture, sur le bureau, sous une pile de magazines, chez le docteur, dans un bar ou tout simplement dans une poche de pantalon dans le panier à linge sale. Si en plus, il est sur vibreur

ou silencieux, c'est la catastrophe. L'application Lookout, comme ses principales concurrentes, propose un service de localisation de votre appareil. Il est ici gratuit, pas besoin de passer à la caisse et à la version Premium. Vous disposez néanmoins d'un délai de 2 semaines après installation pour profiter de toutes les fonctionnalités : alertes antivol (avec photo du voleur), verrouillage à distance, etc.



PROTECTION

Vol ou perte de smartphone

RETROUVEZ VOTRE TÉLÉPHONE PERDU AVEC LOOKOUT

PRATIQUE

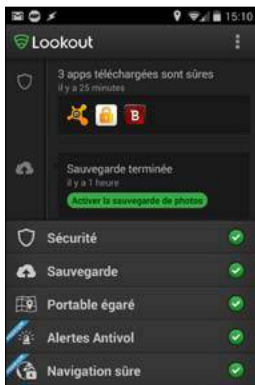


01 > INSTALLATION

En premier lieu il faudra installer

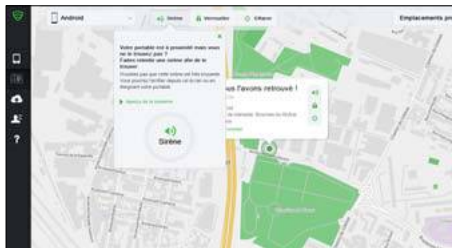
l'appli **AntiVirus & Sécurité** |

Lookout et se créer un compte lors du premier lancement. Lorsque votre téléphone est perdu, rendez-vous sur le site **www.lookout.com** et connectez-vous avec vos identifiants. Dans l'onglet **Sauvegarde** vous aurez l'occasion de récupérer les principales données contenues dans votre téléphone.



03 > ILA SIRÈNE

Si le GPS est activé, la précision de la localisation peut aller jusqu'à une dizaine de mètres. C'est parfois insuffisant pour le retrouver. En cliquant sur l'option **Sirène**, vous le ferez sonner, et ce, même s'il est en mode silencieux ou en veille. La manipulation ne fonctionnera pas si le smartphone est éteint ou en mode avion. Malheureusement l'alerte antivol (qui sonne lorsque votre appareil se situe à X mètres de vous) ne fonctionne qu'avec la version payante.



02 > LOCALISER VOTRE TÉLÉPHONE

Dans l'interface Web de Lookout, cliquez sur l'onglet **Localiser mon portable** pour ouvrir la carte et tenter de retrouver votre appareil



(fonctionne aussi avec les tablettes). Il faudra cependant que celui-ci soit chargé et connecté à Internet, d'une manière ou d'une autre (3G ou WiFi). Bien sûr cela fonctionne avec tous vos appareils enregistrés.

MCAfee, UN BON CHOIX AUSSI

À l'instar de l'application Lookout, McAfee propose aussi un mode antivol dans son application dédiée à la sécurité. Ici aussi il faudra se créer un profil en ligne. Cela vous permettra d'enregistrer vos différents appareils et, si jamais l'un d'eux se fait voler, vous pourrez le retrouver en accédant à votre compte. De même, vous devrez associer un code PIN à votre compte qui vous servira au moment de déverrouiller l'un de vos appareils. La création d'un compte vous permet aussi de sauvegarder vos données personnelles.

Lien : www.mcafeemobilesecurity.com





CRYPTTEZ TOUT CE QUE VOUS METTEZ SUR VOTRE CLOUD !

UN CLOUD C'EST TRÈS BIEN SAUF QUAND LA NSA VIENT VOIR CE QUE CONTIENNENT VOS FICHIERS OU LORSQU'UN PIRATE PARTAGE LES PHOTOS DE VOS FESSES AVEC LE MONDE ENTIER. SI VOUS UTILISEZ DROPBOX, ONEDRIVE OU GOOGLE DRIVE POUR STOCKER VOS DOCUMENTS OU PHOTOS DE FAMILLE, IL SERAIT PEUT-ÊTRE TEMPS DE CHIFFRER TOUT ÇA...



DES FICHIERS PERSONNELS À L'ABRI

Si vous avez un appareil Android, iOS ou même Windows Phone il existe BoxCryptor, une application permettant de chiffrer en AES256 vos documents et de les envoyer sur le service de stockage de votre choix (voir encadré). Une fois sur votre cloud, même si un petit curieux met son nez dans votre compte il ne pourra savoir de quoi il retourne. Alors bien sûr, BoxCryptor n'a pas que des avantages : l'appli est payante si vous utilisez plus de deux appareils ou si vous utilisez plus d'un hébergeur. Les sources ne sont pas non plus disponibles ce qui est rédhibitoire pour les professionnels.

Depuis les révélations d'Edward Snowden sur les petites habitudes de la NSA, on sait bien qu'il est impossible de faire confiance aux services qui stockent vos fichiers. La solution consiste alors à utiliser TrueCrypt ou VeraCrypt pour placer un conteneur chiffré sur votre cloud et aller piocher dedans ou ajouter des éléments lorsque vous le désirez. Le problème c'est que ces logiciels n'existent pas sur mobiles.



Une des solutions les plus simples et «tout-en-un» pour les possesseurs de mobiles



Pas «open source» et certaines options payantes (36 €/an)



PREMIERS PAS AVEC BOXCRYPTOR

PRATIQUE



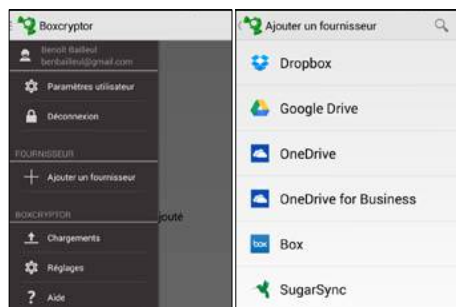
01 > INSTALLATION

Passez la présentation en faisant défiler vers la droite et ouvrez-vous un compte en appuyant sur **S'inscrire**. Renseignez les champs et confirmez que vous comprenez les risques du chiffrement en cochant la case (si vous perdez votre mot de passe, BoxCryptor ne pourra pas vous le rendre). Confirmez l'utilisation de BoxCryptor depuis votre boîte aux lettres.



02 > LE FOURNISSEUR

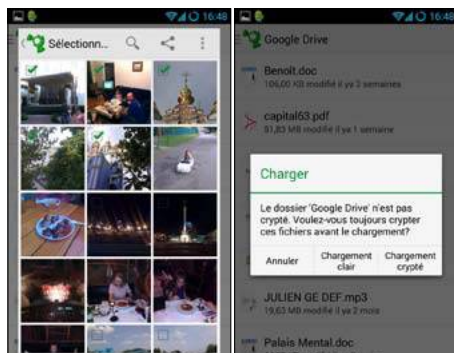
Depuis le panneau latéral (un appui sur le logo **BoxCryptor**), faites **Ajouter un fournisseur**. Dans notre cas nous avons choisi Google Drive mais vous en trouverez une vingtaine d'autres. Vous verrez alors les dossiers/fichiers déjà présents sur



votre cloud. Attention ces derniers ne seront pas chiffrés automatiquement. N'oubliez pas de valider cette nouvelle activité sur votre compte mail (par exemple Google vous demandera si vous êtes bien à l'origine de cette connexion).

03 > UPLOAD DES FICHIERS

En bas de l'interface, vous trouverez un petit bouton pour uploader. Choisissez de quel type de fichier il s'agit et sélectionnez-les dans la liste.



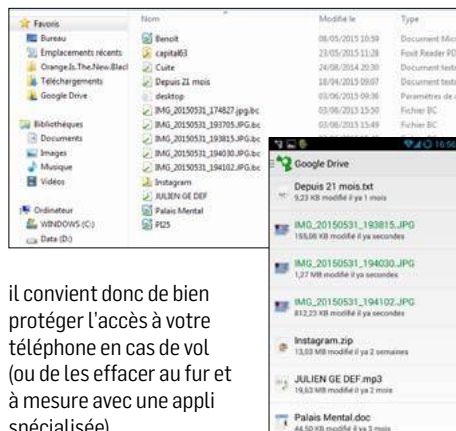
Choisissez le **Chargement crypté** et vos fichiers (ici des photos) iront dans votre compte Google Drive. Attention, ils ne seront pas protégés en écriture (un pirate pourra les effacer).

04 > ATTENTION À LA SÉCURITÉ!

Notez que dans la version gratuite, les noms des fichiers ne sont pas chiffrés: nos photos apparaîtront donc en tant que **XXXXX.JPG.bc**. Bien sûr vous pourrez les renommer pour brouiller les pistes. Sans votre mot de passe, un pirate qui aura accès à votre compte Google ne pourra pas les afficher. Par contre sur votre appareil, les photos ne seront pas chiffrées à leur emplacement d'origine,

**INFOS [BOXCRYPTOR]**Où le trouver ? [www.boxcryptor.com]

Difficulté :



il convient donc de bien protéger l'accès à votre téléphone en cas de vol (ou de les effacer au fur et à mesure avec une appli spécialisée).

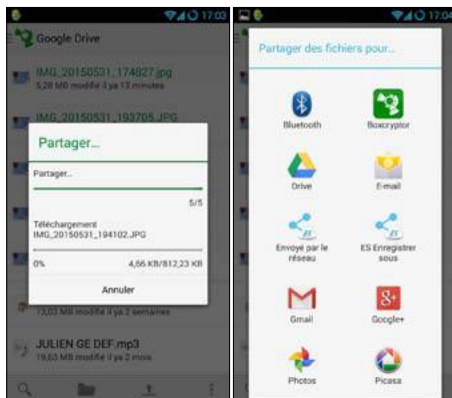
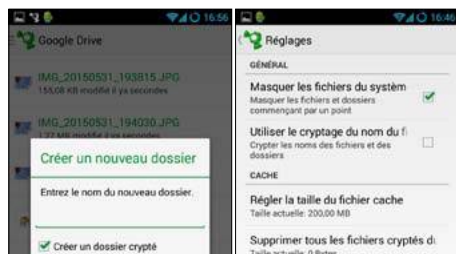
possibilité de créer un **Dossier crypté**. Pour accéder à ces fichiers/dossiers cryptés depuis un autre appareil, il suffit d'installer BoxCryptor sur votre PC, Mac ou un autre appareil compatible muni de vos identifiants.

06 > LE PARTAGE

Pour partager vos photos avec d'autres personnes, il suffit de les sélectionner dans l'interface et de sélectionner l'icône partage (les trois petits points reliés par deux traits). BoxCryptor ira déchiffrer les fichiers à la volée et vous proposer une liste d'applis installées: Gmail, Whatsapp, Bluetooth, Facebook, etc. Vos amis recevront les fichiers «en clair».

05 > SUR D'AUTRES APPAREILS

Pour plus de clarté entre les documents chiffrés et ceux qui ne le sont pas, vous avez la



LES SERVICES DE CLOUD COMPATIBLES

BoxCryptor est compatible avec une vingtaine d'hébergeurs dont certains sont presque inconnus. Vous trouverez la liste à cette adresse : www.boxcryptor.com/fr/provider. Ci-dessous les clouds les plus utilisés en France... Vous disposez d'un NAS à la maison ? BoxCryptor le prendra aussi en charge !

Dropbox : www.dropbox.com/frSugarSync :
www.sugarsync.comGoogle Drive :
<https://drive.google.com>Box.net :
www.box.netMicrosoft OneDrive :
<https://onedrive.live.com>

CHEZ VOTRE MARCHAND
DE JOURNAUX

PRIX MINI
2,90€

SAMSUNG » NEXUS » HTC » LG » SONY » WIKO » ETC.

Android

Mobiles & Tablettes



AVR.-JUIN 2015

BEST-OF **APPLIS & ASTUCES**

Le **GUIDE**
SMARTPHONE
100% GRATUIT

TOUT FAIRE AVEC SON MOBILE



SÉCURITÉ

CES FAILLES QUI MENACENT
VOS DONNÉES PRIVÉES...

Nos solutions
pour se protéger



60 FICHES
PRATIQUES

- » Vie pratique
- » **BOOSTER L'AUTONOMIE**
- » Gérer ses mails



MINI PRIX
2,90€
seulement

LE 1^{ER} MAGAZINE
100% ANDROID ET 100% PRATIQUE



INFOS [AVAST! SECURELINE VPN]

Où le trouver ? [<http://goo.gl/oc02qW>]

Difficulté : ☹️☹️☹️

PROTÉGEZ VOTRE MOBILE & SURFEZ ANONYMEMENT

VOUS CONNAISSEZ LES VPN SUR PC ? ILS VOUS PROTÈGENT DES PIÈGES ET DES MALWARES LORSQUE VOUS SURFEZ SUR DES HOTSPOT PUBLICS. SUR MOBILE C'EST PAREIL ! AVAST! SECURELINE VPN VOUS PROPOSE DONC DE SURFER SUR LE WEB DE MANIÈRE SÉCURISÉE ET ANONYME, TOUT EN ACCÉDANT À DU CONTENU GÉOLOCALISÉ.

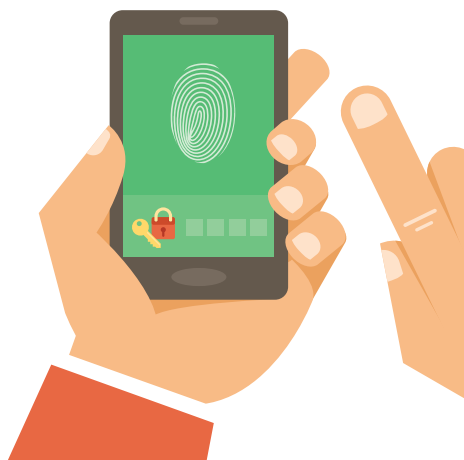


Facile à mettre en place pour les débutants



Au bout de 7 jours, vous devrez ouvrir le porte-monnaie... ou choisir une autre appli !

Espionnage de la NSA, piratage des données, anonymat relatif... Surfer sur Internet n'est pas sans danger, surtout sur smartphone où l'on se connecte souvent à des points Wi-Fi publics non sécurisés. Une solution pour y remédier : passer par un VPN, ou Virtual Private Network, comme SecureLine d'Avast!. Le principe est simple. Une fois le VPN activé, les données envoyées quand vous serez sur Internet passeront par un «tunnel» où elles seront cryptées, rendant impossible l'espionnage de vos données. L'appli étant associée à un proxy, vous pourrez apparaître comme résident d'un autre pays que le vôtre. Enfin, l'application peut s'activer automatiquement lors d'une connexion à un Wi-Fi public ou au(x) réseau(x) de votre choix. Concrètement, SecureLine VPN vous permettra de surfer sur le Web de manière anonyme et sécurisée, et de télécharger des applications normalement inaccessibles en France (Hulu,



Pandora, etc.) A l'inverse si vous voyagez souvent à l'étranger, sachez qu'utiliser Avast! SecureLine VPN permettra d'accéder à du contenu Web géographiquement limité à la France (le VPN est disponible dans la version payante). Niveau tarif, vous disposez d'une période d'essai de 7 jours. Passé ce délai, SecureLine VPN vous coûtera 2,59 € par mois ou 19,99 € par an.



PROTECTION VPN

COMMENT PARAMÉTRER AVAST! SECURELINE VPN

PRATIQUE



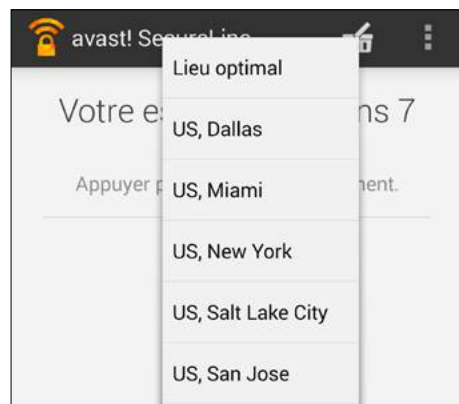
01 > LANCEMENT DU VPN

Une fois l'application ouverte, appuyez sur **Continuer** (2fois) puis sur **Continuer vers l'application**. Une fois sur la page principale d'Avast! SecureLine VPN, faites glisser le bouton vers le haut (**Activé**) et cocher la case **J'ai confiance en cette application**. Validez avec **OK**, attendez que la connexion se fasse et terminez avec **Fermer**.



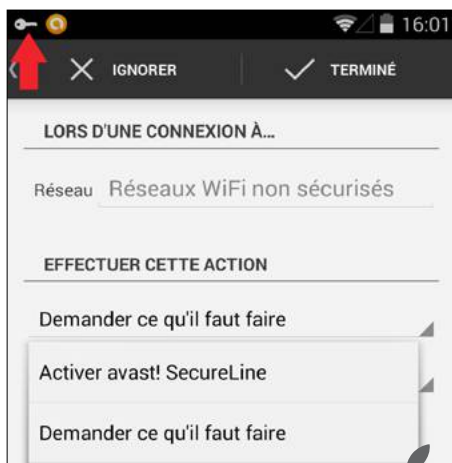
02 > CHOISIR SON PROXY

Pour accéder à du contenu uniquement accessible dans certains pays, il faudra parfois choisir un proxy particulier. Sur la page principale de l'application, touchez la ville indiquée en bas de l'écran (à droite de **Lieu**). C'est là que vous pourrez choisir parmi 11 villes, réparties entre les USA, la Grande-Bretagne, l'Allemagne, Singapour, la République tchèque, etc.



03 > PARAMÉTRER L'UTILISATION AUTOMATIQUE DU VPN

Pour qu'Avast! SecureLine VPN s'active automatiquement (ou non) lors d'une connexion à un réseau Wi-Fi public ou celui de votre choix, touchez les trois points verticaux puis **Règles de connexion**. Appuyez sur **Demander ce qu'il faut faire** puis **Activer Avast! SecureLine VPN** pour automatiser son utilisation par exemple. De la même manière, définissez le proxy.



VPN EXPRESS

Compatible

Cette appli pour iPhone et iPad permet de se protéger lorsque vous utilisez un réseau sans fil qui n'est pas sécurisé. Vous aurez le droit à 300 Mo de trafic journalier gratuit !

Lien :
<http://goo.gl/Rmkunf>





INFOS [DASHLANE] Difficulté :

Où le trouver ? [<http://goo.gl/ECcmX> (Android)]

Où le trouver ? [<http://goo.gl/zHFOA> (iOS)]

Dashlane :

VOTRE MOT DE PASSE PRINCIPAL



SI VOUS ÊTES FAMILIER AVEC LE CONCEPT DE MOT DE PASSE PRINCIPAL, RÉJOUISSÉZ-VOUS ! L'APPLICATION DASHLANE DISPONIBLE SUR ANDROID ET iOS PERMET DE CENTRALISER TOUS VOS SÉSAMES. TOUS VOS AUTRES MOTS DE PASSE SERONT ENREGISTRÉS SANS AVOIR À LES MÉMORISER OU LES TAPER.



Un chiffrement local solide (AES 256) et la possibilité de sauvegarder d'autres données confidentielles



Passé 30 jours, il faudra acheter une licence pour continuer à synchroniser ses mots de passe

Le risque sur Internet c'est de négliger la sécurité de ses mots de passe. On est souvent tenté de «recycler» ses mots de passe lors d'une nouvelle inscription sur un site. Si un hacker découvre votre sésame «toto» valable pour le site A, il découvrira ceux des sites B, C et D si vous avez choisi «toto75», «ToTo», «Totobogoss», etc. La solution pour éviter de tout retenir est de choisir un mot de passe principal qui débloquera tous les autres. Dashlane propose en effet de saisir vos mots de passe vers Facebook, Gmail ou Instagram puis de les retenir en local dans un coffre fort numérique crypté.

DASHLANE VA PLUS LOIN

Dashlane fait encore plus puisqu'il permet de remplir automatiquement des formulaires d'inscription, d'enregistrer des documents confidentiels comme votre carte de sécurité sociale, passeport, carte d'identité, numéro de carte bancaire, etc. Pas de risque au niveau de la sécurité puisque le mot de passe qui déverrouillera tout ça doit obligatoirement comporter 8 caractères avec chiffres, minuscules et majuscules. Petite précision : tout est stocké en local, votre mot de passe ne se baladera pas dans un «cloud» ou un serveur distant...



PROTECTION

Mot de passe

ENREGISTREZ VOS SÉSAMES

PRATIQUE



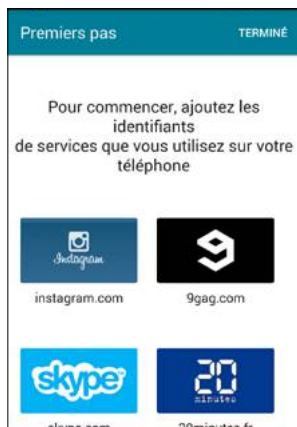
01 > VOTRE MOT DE PASSE «MAÎTRE»

Après avoir installé et démarré l'appli, passez la présentation et appuyez sur **Continuer**. Faites **Créer un compte**. Ce dernier devra comporter 8 caractères, au moins une lettre et un chiffre, au moins une majuscule, etc. Si un critère n'est pas rempli, vous ne pourrez pas sauver vos mots de passe. En effet ce mot de passe maître servira à déverrouiller tous les autres (mais vous pourrez par la suite créer un code PIN plus rapide à saisir).



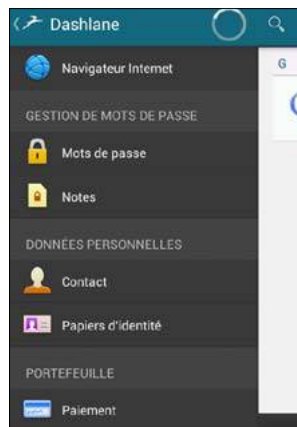
02 > VOS SITES PRÉFÉRÉS

Lorsque l'appli affichera que le compte a bien été créé, faites **Démarrer** et commencez à sélectionner un des sites auquel vous êtes habitué dans la liste. Si un de vos sites ne figure pas dans la liste, vous pourrez rentrer l'URL à la main plus tard. Faites **Terminer** et remplissez les champs **Identifiant** et **Mot de passe**. À l'avenir, si Dashlane est activé sur votre appareil vous n'aurez pas à rentrer cet identifiant. Continuez avec vos autres sites favoris...



03 > LES AUTRES FONCTIONNALITÉS

Dashlane fait aussi office de coffre fort numérique. En effet vous pourrez mettre les informations concernant votre passeport, votre carte vitale, votre compte Paypal ou les numéros de votre carte bancaire. Tout sera débloquable avec votre mot de passe maître. Heureusement tout cela est chiffré en AES 256 bits. Allez dans le menu déroulant de gauche et faites **Pièces d'identité**, **Données personnelles** ou **Paiement**.



30 JOURS D'ESSAI POUR LA VERSION PREMIUM

Lorsque vous installerez Dashlane vous aurez automatiquement accès à la version Premium pendant 30 jours. Cette dernière permet de synchroniser vos identifiants entre les différentes versions de Dashlane qui équipent vos appareils. Pas besoin de retaper tous vos mots de passe si vous voulez que vos identifiants soient disponibles du PC, sur votre tablette ou votre téléphone... Passé ce délai, il faudra payer 40€/an pour pouvoir accéder aux mots de passe depuis le site Web ou profiter de la synchronisation avec vos autres appareils.



INFOS [Secrecy]

Où le trouver ? [<http://goo.gl/ONOsSE>]

Difficulté : 



VOS DOCUMENTS DANS UN COFFRE FORT

IL EXISTE PLUSIEURS SOLUTIONS POUR METTRE À L'ABRI SES DOCUMENTS, MAIS RARES SONT LES APPLIS QUI PERMETTENT DE LA FAIRE SANS «ROOT». SECRECY PERMET DE CRYPTER N'IMPORTE QUEL TYPE DE FICHER SANS DEMANDER DE COMPÉTENCES PARTICULIÈRES ET SANS MODIFICATION SUR VOTRE SMARTPHONE OU TABLETTE...



L'ajout de Secrecy dans les menus contextuels d'Android



Le mode furtif est payant

Sur le Play Store vous trouverez facilement des applis permettant de masquer des documents, mais il existe toujours un hic : prise en charge de certains types de fichier uniquement, «root» systématique, problème de sécurité (fichiers temporaires résiduels), chiffrement inexistant ou faible, etc. Secrecy propose une solution simple et open source. Il suffit de se confectionner un espace chiffré en AES 256 où vous pourrez placer vos documents sensibles. Personne ne pourra accéder à vos photos,

vidéos, PDF et autres fichiers. Vous choisissez l'emplacement de ce coffre fort (mémoire interne ou carte SD) et la sélection des fichiers se fait via le menu partage qui est commun à toute les applications. Si vous désinstallez Secrecy ou que vous exportez vos contenus chiffrés vers un PC par exemple vous pourrez les déchiffrer avec un logiciel compatible AES 256 comme 7Zip. Seule ombre au tableau, le mode furtif est payant. Il faudra faire un don pour masquer Secrecy de la liste des applications installées.



PROTECTION

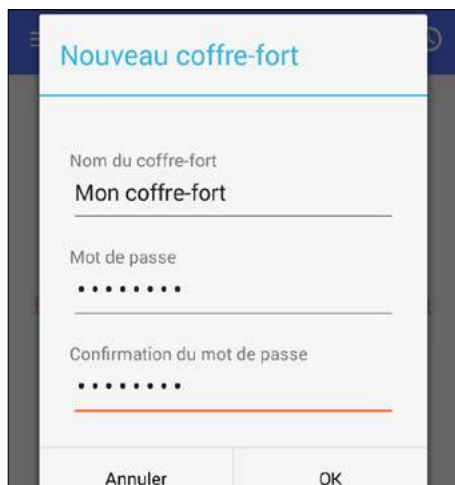
Chiffrement

PRISE EN MAIN DE SECRECY

PRATIQUE



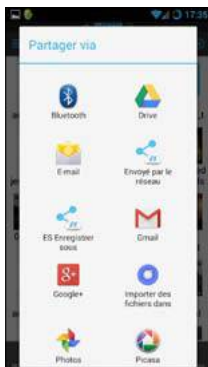
01 > VOTRE CONTENEUR
Après l'installation, sélectionnez le + en haut et choisissez un nom pour votre premier coffre fort. L'appli vous demandera de choisir un mot de passe. Le chiffrement se fait un peu à la



manière de TrueCrypt sauf qu'ici il n'y a pas de limite d'espace à votre conteneur protégé. Validez.

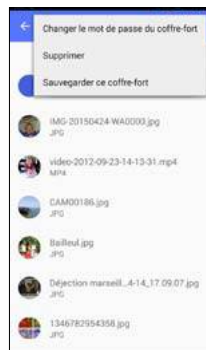
02 > LES FICHIERS

Pour sélectionner un ou plusieurs fichiers, il suffit d'utiliser le menu contextuel d'Android. Dans une application comme **Galerie** ou un gestionnaire de fichiers, faites **Partager** (ou **Share**) et choisissez **Importer des fichiers dans Secrecy**. Trouvez votre coffre-fort et validez.



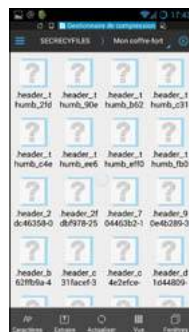
03 > LES PARAMÈTRES

Il est possible de faire une sauvegarde de votre coffre fort et d'avoir un aperçu. Dans les **Paramètres** vous pourrez faire un don pour profiter du mode furtif et changer l'emplacement de sauvegarde. Notez que si vous décidez de restaurer les fichiers pour les afficher «en clair» ils ne reprendront pas forcément place à leur emplacement d'origine.



04 > ATTENTION!

Si vous faites un tour dans le dossier **SECRECYFILES**, vous n'y verrez que les versions chiffrées de vos fichiers. Il est possible d'exporter l'archive pour pouvoir les déchiffrer depuis un PC mais surtout n'oubliez pas votre mot de passe, car il vous serait impossible de récupérer vos fichiers!



ET SUR IPHONE ?

Compatible

Sur iPhone il existe l'application **Best Secret Folder** qui permet de cacher photos et vidéos dans un dossier spécial protégé par mot de passe. Pas de chiffrement au programme, mais c'est mieux que rien n'est-ce pas ?

Lien : <http://goo.gl/jYQ13E>



ÊTES-VOUS SUR ÉCOUTE ?

VOUS PENSIEZ QUE LES MISES SUR ÉCOUTES TÉLÉPHONIQUES SONT RÉSERVÉES AUX CRIMINELS ET QU'IL FAUT ABSOLUMENT DEMANDER L'AUTORISATION D'UN JUGE ? C'EST FINI TOUT ÇA ! AVEC LA LOI SUR LE RENSEIGNEMENT, N'IMPORTE QUEL CITOYEN PEUT DEVENIR LA CIBLE DES IMSI CATCHER. CES FAUSSES ANTENNES RELAIS QUI TIENNENT DANS UNE VALISE PEUVENT INTERCEPTER SMS ET CONVERSATION. VOYONS COMMENT LES CONTOURNER...



Malgré son interface complexe, IMSI Catcher Detector n'est pas réservé aux experts de la téléphonie



Des bugs sur certaines machines car l'appli est encore en version «alpha»

Le problème avec le protocole GSM c'est que son chiffrement ne tient pas la route. Les autorités peuvent écouter nos téléphones mobiles en coopérant avec les compagnies téléphoniques, mais depuis la loi sur le Renseignement, la police ne prend même plus la peine de demander la permission. Avec un appareil spécifique tenant dans une valise appelé IMSI Catcher, la police ou les services secrets peuvent faire croire aux téléphones mobiles des environs (la portée est variable et dépend du type d'appareil) qu'il s'agit d'une antenne relais de confiance. Une fois que le téléphone cible accepte le IMSI-catcher en tant qu'antenne,



le chiffrement GSM peut être tout simplement désactivé ! Bien sûr l'utilisateur n'est prévenu de rien et voilà que ses conversations ont aussi publiques que s'il parlait dans un talkie-walkie à 10 €. Vous pouvez bien sûr ajouter une couche de chiffrement avec Discretio par exemple (voir *Guide du Pirate* n°1 ou *Pirate Informatique* n°17), mais tout le monde de dispose pas de ce type de logiciel. IMSI Catcher Detector vous préviendra d'un risque en analysant en temps réel le réseau...



Voilà ces fameux IMSI Catcher utilisés par les criminels...et par nos chers dirigeants !



PROTECTION

Anti-surveillance

COMMENT FONCTIONNE IMSI CATCHER DETECTOR ?

PRATIQUE



01 > INSTALLATION

Suivez notre lien et téléchargez le fichier **Android-IMSI-Catcher-Detector.apk**. À vous de voir comment procéder ensuite: soit vous transférez le fichier sur votre smartphone via USB ou vous faites comme notre rédacteur en chef (qui ne trouve jamais son fichu câble) et vous vous envoyez le fichier APK à vous même par e-mail... Installez l'appli. Il faudra

bien sûr autoriser les **Sources inconnues** depuis **Paramètres > Sécurité**.

02 > VOTRE CLÉ

L'appli vous demandera ensuite d'activer le GPS pour connaître votre localisation. Elle s'ouvrira ensuite sur l'onglet **Phone/SIM Details**. Allons dans le menu en sélectionnant l'icône en haut à gauche puis allez dans **Préférences**. Ici vous pourrez demander une OpenCellID API Key permettant de télécharger la base de données des antennes environnantes (**Request OCID API Key**). Attendez quelques secondes, redémarrer l'appli et faites ensuite **Open-CellID API Key**. Votre clé unique devrait normalement s'afficher dans le champ. Faites **OK**.

03 > LA CARTE

Vous pourrez alors télécharger les emplacements d'antennes dans le secteur (**Download Local BTS Data**) puis aller dans **Antenna Map**

Viewer pour voir où sont ces antennes sur la carte. Ici il existe un code couleur pour connaître le risque (voir encadré). Dans notre petite ville test, le risque n'est pas énorme, mais deux antennes sont en orange. Il peut s'agir de faux positif, mais mieux vaut être prudent!



04 > LES OPTIONS

Il est possible de télécharger d'autres données moins indispensables dans l'onglet **Database Viewer**. Vous trouverez un glossaire des termes techniques ici: <http://goo.gl/aw2H3o>.



Dans les **Préférences** vous pouvez faire en sorte de démarrer l'appli automatiquement lorsque le téléphone s'allume (**Auto Start**) ou d'utiliser le **Persistent Service** pour continuer de scruter le réseau même si l'appli n'est pas chargée.

LE CODE COULEUR

	Normal	Pas de menace détectée. Le réseau utilise au moins l'algorithme A5/3
	Risque moyen	Au moins une antenne du réseau est inconnue ou utilise un chiffrement inférieur au A5/3
	Risque fort	Un IMSI Catcher a été détecté et scanne les environs
	Dangereux	L'IMSI Catcher est en train de vous tracker. Partez ou cessez de communiquer.
	Courrez !	Vous étiez déjà la cible mais là, un pirate essaye de manipuler votre téléphone à distance !



INFOS [Google+]

Difficulté : ☠☠☠



EMPÊCHER LES applications d'accéder À VOTRE COMPTE GOOGLE+

SANS QUE VOUS EN SOYEZ INFORMÉ, VOS APPLICATIONS TRANSMETTENT VOS MOINDRES FAITS ET GESTES À VOTRE COMPTE GOOGLE+, QUI DEVIENT UNE VÉRITABLE VITRINE DE L'ENSEMBLE DE VOS ACTIVITÉS SUR ANDROID.

Certaines applications que vous téléchargez sur le Play Store sont associées à votre compte Google+. Concrètement, cela leur donne la permission d'interagir avec le réseau social de Google. Depuis 2012, la firme a décidé de jouer «corporate» : la plupart de ses services laissent une trace sur votre compte Google+. Le meilleur exemple de la volonté de l'entreprise de Larry Page de donner une importance à son réseau social est la création automatique d'un profil Google+ dès la mise en service d'un compte Google ou YouTube. Mais les services officiels de la firme ne sont pas les seules à avoir accès à votre profil,

d'autres applications, à l'instar de SoundCloud ou 8tracks, le font également. Sur Android, le problème est d'autant plus grave qu'un compte Google est obligatoire pour pouvoir profiter de l'ensemble des fonctionnalités de votre smartphone : vous êtes donc obligatoirement le propriétaire involontaire d'un compte Google+. Le réseau social devient une vitrine de l'ensemble de vos activités qui y sont affichées de manière automatique. S'il est (trop) simple d'associer des jeux et des applications à votre profil Google+, les dissocier est une autre paire de manches. Plongée au cœur des paramètres de ce réseau social qui ne vous veut pas que du bien.



PROTECTION

Google+

DISSOCIEZ VOS APPLIS DE GOOGLE+

PRATIQUE



01 > ACCÉDER À LA LISTE DES APPLICATIONS

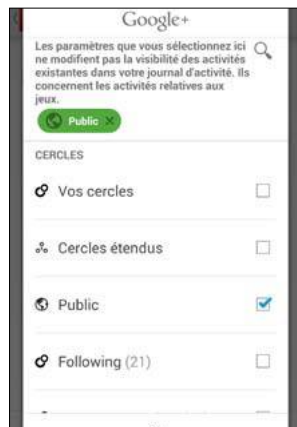
Une fois connecté à votre compte Google+, touchez les trois points en haut à droite de votre écran. Sélectionnez **Paramètres** puis, dans **Paramètres du compte**, touchez votre adresse mail. Dans la nouvelle fenêtre, entrez dans **Apps avec Google+ Sign-In**, vous avez alors devant vous la longue liste de toutes les applications qui sont associées à votre compte.

02 > DISSOCIER TOTALEMENT UNE APPLICATION D'UN COMPTE

Touchez l'application que vous souhaitez dissocier de votre compte Google+. Vous voyez alors toutes les données que l'application transmet à votre profil. Touchez simplement **Dissocier** pour que cette dernière ne communique plus avec Google+. N'oubliez pas de cocher **Supprimer également toutes vos activités sur Google**, les informations transmises jusqu'à présent seront effacées.

03 > DISSOCIER EN PARTIE UNE APPLICATION D'UN COMPTE

Si vous souhaitez annuler seulement une partie des données transmises automatiquement à votre compte Google+, il vous suffit de toucher l'un des paramètres, et de suivre les instructions. Par exemple, si vous ne voulez plus que votre historique de connexion à une application soit public, sélectionnez-la puis, touchez **Pers. pouvant voir que vous êtes connecté**. Dans la nouvelle fenêtre, touchez la croix à côté de **Public** et validez avec **OK**. Votre historique de connexion est désormais privé.



300 MILLIONS

C'est le nombre d'utilisateurs actifs de Google+ à travers le monde, ce qui le place à la deuxième place des réseaux sociaux les plus populaires, devant Twitter et ses 271 millions de twittos, mais très loin derrière Facebook et son 1,32 milliard d'utilisateurs actifs.



INFOS [ORBOT]

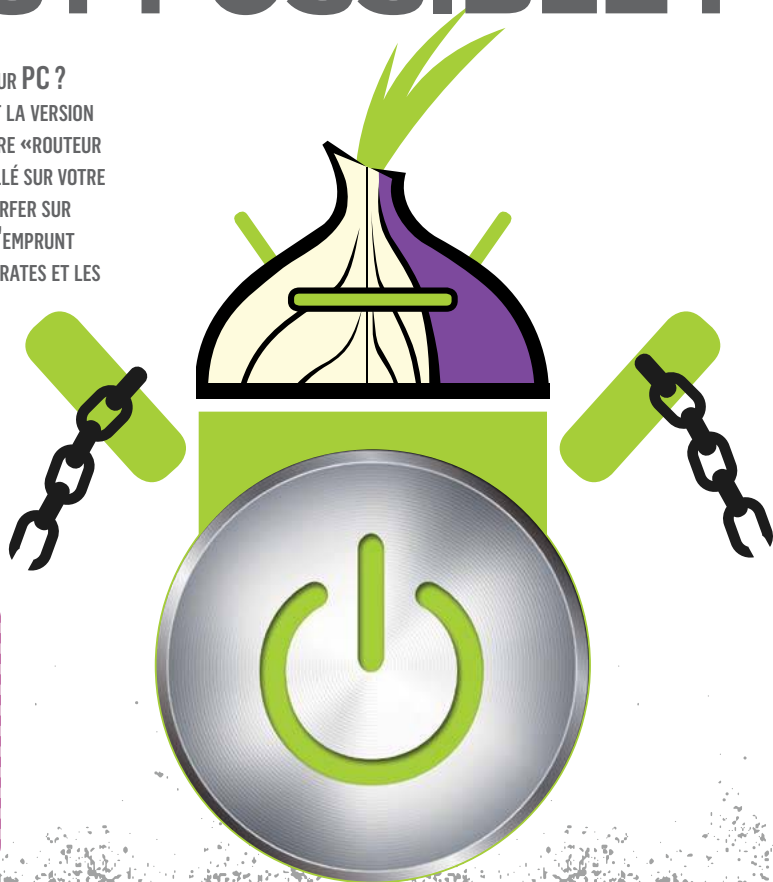
Où le trouver ? [<http://goo.gl/vwUcpR>]

Difficulté : ☠ ☠ ☠

TOR sous ANDROID : C'EST POSSIBLE !

VOUS CONNAISSEZ TOR SUR PC ?

ORBOT TOUT SIMPLEMENT LA VERSION POUR ANDROID DU CÉLÈBRE «ROUTEUR ONION». UNE FOIS INSTALLÉ SUR VOTRE MOBILE VOUS POURREZ SURFER SUR INTERNET SOUS UNE IP D'EMPRUNT POUR CONTOURNER LES PIRATES ET LES ESPIONS. AVEC UN MOBILE ROOTÉ, C'EST MÊME L'INTÉGRALITÉ DE VOTRE TRAFIC INTERNET QUI VA PASSER PAR LE PROTOCOLE DE TOR...



Gratuit



Un appareil rooté est nécessaire pour faire transiter tout le trafic



Tor est un réseau informatique décentralisé qui utilise une architecture en oignon (d'où le logo). Le système est composé de routeurs organisés en couches. Les paquets de données transitent d'un routeur vers un autre en laissant peu de traces sur leur origine. Même s'il est théoriquement possible de tracer un utilisateur (nous ne sommes jamais à 100 % anonymes), il est très difficile de le faire, car chaque routeur ne possède que peu d'information sur son successeur et son prédécesseur. Orbot propose aux utilisateurs d'appareils Android d'utiliser le protocole Tor pour surfer en toute sécurité et contourner

les limitations liées à votre réseau (sites interdits ou géolocalisés). Pour ne pas trahir votre position et votre véritable IP il faudra cependant garder en tête que sur les appareils non rootés (voir page 6 et 12), seul le trafic qui passe par votre navigateur est pris en charge par Tor. Mais voyons comment utiliser Orbot au quotidien...



**DEVENEZ
COMPLÈTEMENT
ANONYME AVEC ORBOT**

UN VPN OU TOR ?

Nous avons vu à la page 48 comment fonctionne un VPN sous Android. Tor propose à peu près le même type de service. Ce petit tableau va vous permettre de choisir entre les deux solutions en fonction de vos attentes.

	VPN	Tor
Avantages	- Chiffre tout le trafic - Fonctionne avec tous types d'appareils (rootés ou non) - Relativement plus rapide que Tor	- Communication presque impossible à intercepter car complètement décentralisé - Gratuit
Inconvénients	- Payant (ou limité si gratuit) - Centralisé donc potentiellement «espionable»	- Certaines utilisations non prévues peuvent vous rendre «visible» (comme le téléchargement via BitTorrent) - Relativement plus lent qu'un VPN



COMMENT UTILISER ORBOT ?

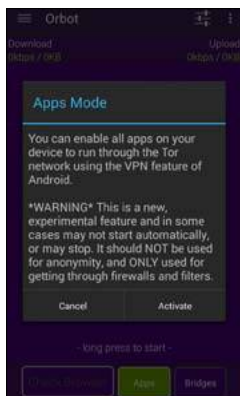
PRATIQUE



01 > PREMIER DÉMARRAGE

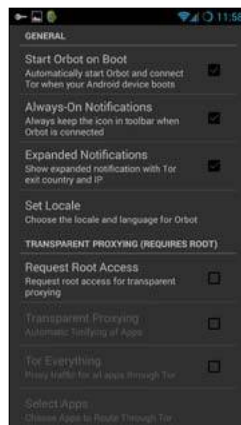
Lors du premier démarrage, choisissez

Apps pour faire passer par Tor tout le trafic Internet qui émane de votre appareil. Si ce dernier est rooté, nous vous le conseillons. Dans le cas contraire, sachez que seul le trafic du navigateur par défaut sera pris en charge. Attention Orbot est encore au stade expérimental : l'application peut s'arrêter ou ne pas démarrer automatiquement. Cocher la case **J'ai confiance en cette application** et validez.



03 > GÉRER LE TRAFIC

Dans les options (en haut à droite), vous pourrez choisir de démarrer automatiquement Orbot avec le téléphone et de faire passer tout le trafic par Tor. Il faudra cocher **Request Root Access, Transparent Proxying et Tor Everything**. Ne touchez au reste des options que si vous savez absolument ce que vous faites. Sachez que Orbot propose d'utiliser Orweb un navigateur proposant des fonctionnalités sympas comme le contrôle des cookies, l'absence d'historique ou le « déguisement » de votre appareil.



02 > VÉRIFIEZ LE NAVIGATEUR

Appuyez ensuite longtemps sur le bouton de démarrage puis attendez que l'appli vous informe que tout s'est bien passé (le robot devrait être vert). Pour vérifier que votre navigateur est bien paré pour une navigation en oignon, faites **Check Browser**. Attention, seul le navigateur par défaut sera testé ! Normalement Orbot devrait afficher une page vous indiquant que la navigation est sans risque.



04 > PROTOCOL OBFUSCATION?

Dans la fenêtre principale, vous verrez aussi l'icône **Bridge**. Si vous êtes dans un pays qui interdit le protocole Tor, il faudra utiliser «un pont» pour mettre un premier pied dans le réseau. Il s'agit du «protocol obfuscation» (**Obfs4**) qui va masquer le protocole en Tor jusqu'au premier «nœud» du réseau. N'utilisez cette option que si vous êtes à l'étranger (Chine, Biélorussie, etc.)





MOUCHARD SUR MOBILE :

COMMENT ÇA MARCHE ? COMMENT S'EN DÉBARRASSER ?



SE FAIRE INFECTER PAR UNE APPLI «ESPIONNE» N'EST PAS DE LA SCIENCE-FICTION. IL EXISTE DE NOMBREUSES SOCIÉTÉS QUI FOURNISSENT CE GENRE DE SERVICE. UNE FOIS QUE LE VER EST DANS LE FRUIT, VOTRE VIE PRIVÉE N'EXISTE PLUS (LOCALISATION DE VOTRE EMPLACEMENT, RÉCUPÉRATION DE VOS SMS, ETC.) COMMENT FONCTIONNE CE TYPE D'APPLI ET COMMENT S'EN DÉBARRASSER ?

Sur le Google Play Store on trouve des applis permettant de surveiller ses enfants ou de contrôler leur mobile à distance. Ces applis s'installent avec une discussion préalable auprès de vos rejetons, mais au final ils ne peuvent pas vraiment s'y opposer : c'est vous qui payez le téléphone, le forfait et ils sont mineurs donc pas

vraiment des êtres humains aux yeux de la loi. À côté de ça il existe aussi d'autres applis qui, elles, ne sont pas disponibles sur le Store officiel, car Google les a bannis. Elle s'appellent MobiPast, OmegaSpy ou TheTruthSpy. Et même si sur leur site nous voyons des familles qui sourient, les enfants ne sont pas du tout la cible : il s'agit ici d'espionner délibérément des individus contre



Très puissant. Version «Standard» gratuite pendant 2 jours



Les antimalwares le détectent sans problème, mais la désinfection n'est pas évidente.



une somme d'argent. Bien sûr c'est illégal, mais pour être inquieté il faut se faire prendre...

COMMENT SE PASSE UNE INFECTION ?

À l'inverse d'un PC sous Windows, vous ne pouvez pas vous faire infecter à distance par ce type de spyware (à moins d'être extrêmement négligent). Le pirate devra avoir accès à votre appareil pendant quelques minutes : ne laissez pas votre téléphone traîner, surtout s'il n'a pas de procédé de verrouillage. Une fois installé, le spyware sera complètement invisible et n'apparaîtra pas dans la liste des applications. Il s'octroiera des privilèges complètement abusifs et prendra un nom qui vous fera hésiter si un antivirus se déclenche. Dans notre exemple, TheTruthSpy va changer de nom pour devenir System Service... Un utilisateur non averti y réfléchira à deux fois avant d'effacer quelque chose avec un nom si «effrayant»...



**UNE FOIS INSTALLÉ,
LE MOUCHARD SERA
COMPLÈTEMENT
INVISIBLE !**

UNE MINE D'INFORMATIONS

De son côté, le pirate pourra avoir accès à une mine d'information à distance depuis une interface Web sur son PC ou sa tablette : contenu des SMS, journaux des discussions, emplacement géographique, contenu des tchats, historiques divers, photos prises, etc. L'appli existe pour iOS (voir encadré) et Android. Vous aurez le loisir d'essayer gratuitement les options les plus basiques pendant 48 heures : géolocalisation, lecture des SMS et journaux d'appels. TheTruthSpy est disponible en trois versions (upgradable sans avoir à réinstaller sur le mobile). Les versions Premium et Gold proposent l'enregistrement des conversations, l'historique du navigateur, le nom des applis utilisées et un accès à Whatsapp. Installer TheTruthSpy sur un téléphone rooté ne sert presque à rien sauf accéder à Hangouts, à l'historique de Skype ou de Facebook. Procédé typique de ce genre d'appli : vous devez payer au mois ! Comptez entre 15 et 20 € pour un mois d'espionnage en fonction de la version que vous avez choisie.

ET SUR LES PRODUITS APPLE ?



TheTruthSpy est aussi disponible sur les produits Apple, mais comme souvent avec ce genre d'application, il faudra que l'appareil soit jailbreaké (voir page 10) pour accéder au marché alternatif Cydia. On imagine pourtant mal une victime ayant ce profil... La version iOS propose à peu près les mêmes options que la version Android sauf que dans la version premium, les appels ne peuvent pas être enregistrés.



PROTECTION

Espionnage

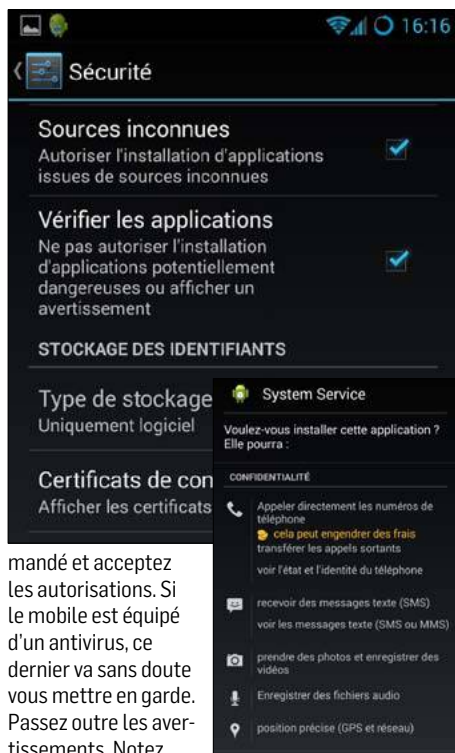
INSTALLER THETRUTHSPY SUR UN MOBILE

PRATIQUE



01 > INSTALLATION

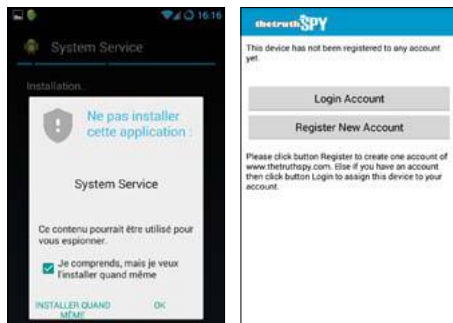
Pour installer l'application, il faudra accepter les **Sources inconnues** dans **Paramètres > Sécurité**. Allez sur le site recom-



mandé et acceptez les autorisations. Si le mobile est équipé d'un antivirus, ce dernier va sans doute vous mettre en garde. Passez outre les avertissements. Notez que vous pouvez installer TheTruthSpy sur trois mobiles différents.

02 > CRÉATION DU COMPTE

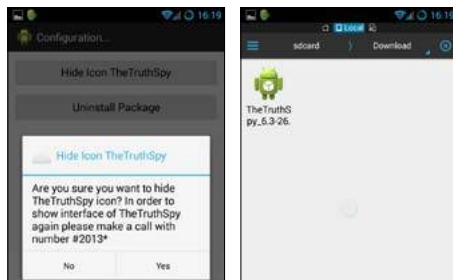
On vous demandera ensuite de créer un compte depuis le téléphone cible (c'est pour cette raison qu'avec cette appli, une contamination à distance est presque impossible). Faites **Register**



New Account et entrez un duo e-mail/mot de passe. Si le téléphone cible est rooté, c'est à ce moment que l'appli vous demandera les droits super-utilisateur (attention ce n'est pas indispensable pour la période d'essai)

03 > CACHEZ L'ICÔNE ET FAITES LE MÉNAGE

Faites ensuite **Configurations** et choisissez bien sûr de cacher l'appli avec **Hide Icon TheTruthSpy**. Pour faire réapparaître l'icône et accéder aux réglages il faudra appeler le numéro **#2013***. Attention cela n'a jamais fonctionné sur notre appareil de test. N'oubliez pas de faire le ménage dans l'historique Web (pour supprimer le lien de téléchargement) et d'effacer le fichier APK du répertoire **Download**. Le téléphone est maintenant piégé!





INFOS [THE TRUTH SPY]

Où le trouver ? [<http://thetruthspy.com>]

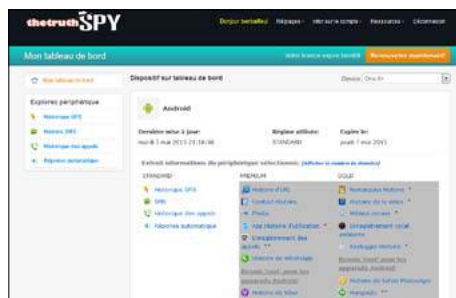
Difficulté :

EXPLOITER THETRUTHSPY À DISTANCE



01 > L'INTERFACE WEB

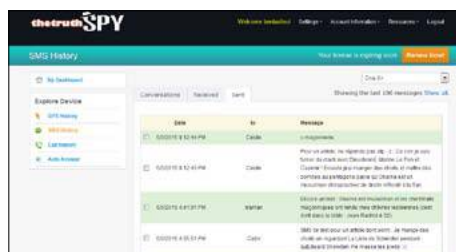
Sur la page du site, faites **Sign In** en haut à droite et entrez les identifiants que vous avez choisis sur le téléphone. Vous voici sur l'interface



principale. Choisissez l'appareil cible dans **Device** et sur le côté gauche choisissez ce que vous voulez analyser dans **Explorez périphérique**.

02 > ACCÈS AUX APPELS ET AUX SMS

Vous pourrez par exemple avoir accès aux SMS du téléphone, y compris ceux qui ont été envoyé avant l'installation de l'appli. Vous aurez bien sûr le numéro de téléphone du destinataire des messages et le nom correspondant dans les contacts. De même vous aurez à disposition la date, l'heure et la durée des appels réalisés avec le téléphone. Ces données peuvent être exportées facilement sur le PC pour y avoir accès hors ligne.



Notez que la version Premium sous Android permet l'enregistrement des appels.

03 > UNE FONCTION RISQUÉE

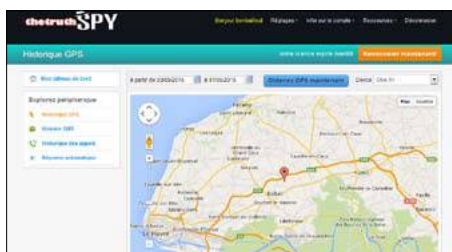
Dans la version Standard il existe aussi une fonction permettant de faire appeler le téléphone cible pour que vous puissiez écouter les sons ambiants. Malheureusement les appels réalisés de cette manière seront visibles sur la



facture. Il s'agit donc d'une méthode risquée en plus d'être peu intéressante (les enregistrements ne font que quelques secondes).

04 > LA LOCALISATION

Bien sûr vous pouvez aussi obtenir la localisation du téléphone. De base l'appli va trianguler la position grâce aux données GSM, mais il est aussi possible d'actionner la fonction GPS à distance sans pour autant l'afficher sur le téléphone. Le service suit à la trace le téléphone: vous pouvez donc savoir où était la personne tel jour ou à telle heure...



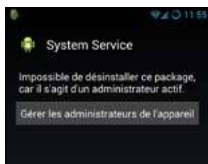


SE DÉBARRASSER DE THETRUTHSPY OU D'UN AUTRE MOUCHARD

UNE APPLI COMME **THE TRUTH SPY** NE FAIT PAS LE POIDS FACE À 80 % DES ANTISPYWARE OU ANTIVIRUS QUE VOUS POURREZ TROUVER SUR LE **GOOGLE PLAY STORE**. MAIS L'APPLI FAIT BIEN LES CHOSSES ET VA S'INSTALLER SOUS LE NOM DE **SYSTEM SERVICE** AVEC UNE ICÔNE GÉNÉRIQUE POUR BROUILLER LES PISTES ET FAIRE CROIRE À UN FAUX POSITIF. DE LA MÊME MANIÈRE **THE TRUTH SPY** VA S'INSTALLER COMME UN ADMINISTRATEUR ACTIF SUR L'APPAREIL. RIEN DE BIEN MÉCHANT, MAIS UN UTILISATEUR LAMBDA N'OSERA PEUT-ÊTRE PAS ALLEZ JUSQU'AU BOUT. VOICI COMMENT FAIRE...

01 > LES ADMINISTRATEURS DE L'APPAREIL

Lorsque votre antivirus ou antispyware aura détecté **System Service** comme étant une menace, choisissez la désinfection ou la désinstallation. Android vous préviendra alors qu'il s'agit d'un administrateur actif. Choisissez de **Gérer les administrateurs de l'appareil...**



02 > BYE BYE!

Vous verrez ici les applis qui disposent de plus de droits que les autres, mais vous retrouverez aussi **Device Admin**. Décochez la case et faites enfin désactiver pour avoir la possibilité de supprimer une bonne fois pour toutes **The Truth Spy**. Bravo votre téléphone est propre maintenant!



	Lookout	Malwarebyte Anti-Malware	Antimouchard Free	NoSpy	AntiSpy	StopSpy
Type	Antivirus	Antivirus	Anti Spyware	Anti Spyware	Anti Spyware	Anti Spyware
Version utilisée	Gratuite	Gratuite	Gratuite	Gratuite	Gratuite	Gratuite
Détection	Oui	Oui	Oui	Oui	Oui	Non
Rapidité	2/5	1/5	5/5	4/5	5/5	Non noté
Interface claire	4/5	1/5	1/5	5/5	1/5	Non noté
Désinfection	Oui (il aura fallu auparavant désactiver le spyware de la liste des administrateurs actifs)	Oui (il aura fallu auparavant désactiver le spyware de la liste des administrateurs actifs)	Non (demande une version payante de l'appli)	Oui (il aura fallu auparavant désactiver le spyware de la liste des administrateurs actifs)	Oui (il aura fallu auparavant désactiver le spyware de la liste des administrateurs actifs)	Non (car pas détecté)
Lien	https://goo.gl/p10c9f	https://goo.gl/x527Fo	https://goo.gl/HMyEz9	https://goo.gl/9YEv6l	https://goo.gl/bmgVfQ	https://goo.gl/JTOjjY
Note	3/5	2/5	1/5	5/5	3/5	0/5



INFOS [CCleaner]

Où le trouver ? [<http://goo.gl/LPrIvs>]

Difficulté : ☠☠☠

NETTOYER SON SMARTPHONE EN PROFONDEUR

TRÈS CONNU SUR PC, CCLEANER A ENFIN DÉBARQUÉ SUR ANDROID ! COMME SON HOMOLOGUE, L'APPLICATION FAIT TRÈS BIEN SON TRAVAIL ET VOUS FACILITE LA VIE AVEC SES NOMBREUSES OPTIONS DE PERSONNALISATION.



Avouez : vous aussi vous êtes du genre à installer tout un tas d'applications pour les tester, avant de les effacer presque aussitôt. L'accès au milliard d'applications du Google Play Store est l'un des plaisirs de posséder un smartphone Android, mais saviez-vous qu'il peut vite devenir un problème ? Chaque fois que vous

installez/désinstallez une appli, elle laisse des fichiers et des dossiers, inutiles et inoffensifs en l'état, mais n'en consommant pas moins votre précieux espace de stockage. C'est là que CCleaner intervient. Une analyse poussée de votre appareil va faire remonter tous les fichiers qu'il est possible d'effacer pour gagner de la place. Complet, intuitif et efficace, CCleaner a tout pour plaire.



Des fonctionnalités avancées en mode «root»



Attention aux mauvaises manipulations !



CCLEANER S'INTÈGRE
PARFAITEMENT DANS
L'ENVIRONNEMENT ANDROID



PROTECTION

Nettoyage

LES FONCTIONS DE CCLEANER

PRATIQUE



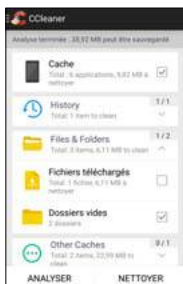
01 > LANCER L'ANALYSE

Ouvrez CCleaner pour arriver directement sur une page résumant l'espace de stockage et la RAM utilisés. Notez que vous pouvez voir également le total de ces deux paramètres, un bon moyen de se rendre compte des différences entre la fiche technique et la réalité. Pour lancer l'analyse, appuyez sur **ANALYSER**.



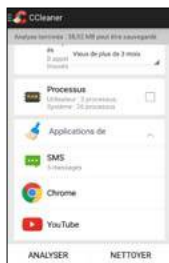
02 > QUE FAUT-IL NETTOYER ?

L'analyse indique en haut l'espace de stockage qu'il est possible de libérer après nettoyage. Cochez ou décochez les dossiers en fonction de ce que vous souhaitez garder. Faites attention, CCleaner peut effacer des fichiers auxquels vous tenez, comme les **Fichiers téléchargés**. Vérifiez bien le tout avant de toucher **NETTOYER**.



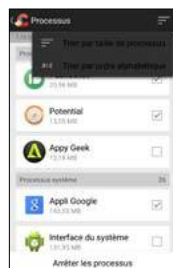
03 > LE NETTOYAGE MANUEL

CCleaner ne peut pas automatiser le nettoyage de certaines applications, qui apparaissent sous **Applications de**. Appuyez sur l'une d'elles, par exemple **SMS**, ouvrez directement l'appli concernée afin que vous puissiez la gérer manuellement. En choisissant **Chrome** ou **YouTube**, vous accédez à la page **Informations sur l'application**, dont vous pourrez **Effacer les données**.



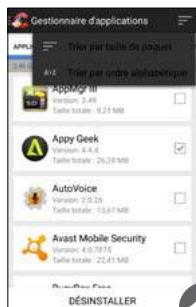
04 > ARRÊTER LES PROCESSUS

Dans les **Infos système**, appuyez sur la case RAM. La liste des processus tournant en fond s'affiche. Si votre appareil est trop lent à votre goût, vous pouvez cocher ceux de votre choix pour libérer la mémoire RAM. Validez avec **Arrêter le processus**. Attention, arrêter certains processus peut causer des dysfonctionnements.



05 > DÉSINSTALLER UNE APPLICATION

Le **Gestionnaire d'applications** de CCleaner (accessible après avoir touché l'icône de l'application) permet de **DÉSINSTALLER** une appli cochée sans passer par la procédure habituelle. Notez que votre téléphone doit être rooté si vous voulez supprimer les **Applications du système**.



SUR IPHONE/IPAD ?

Compatible

Il n'existe pas de CCleaner dans le magasin officiel d'Apple. Pour profiter d'une appli de ce type, il vous faudra un appareil jailbreaké (voir page 10). iCleaner sur le store de Cydia scanne les applications pour supprimer les fichiers inutiles et temporaires, nettoie les cookies et données inutiles de Safari, les journaux, rapports de crash, etc.





RESTAUREZ TOUTES VOS APPLIS



APP BACKUP & RESTORE (CARTE SD)

PRATIQUE



VOUS ABANDONNEZ VOTRE VIEILLE TABLETTE POUR UNE AUTRE ? ON VOUS A OFFERT UN NOUVEAU SMARTPHONE ? POUR RÉCUPÉRER TOUTES VOS APPLIS, LA SOLUTION LA PLUS SIMPLE CONSISTE À PASSER PAR LE GOOGLE PLAY STORE, QUI GARDE EN MÉMOIRE TOUTES VOS INSTALLATIONS. CEPENDANT SI VOUS AVEZ DES APPLIS QUI NE VIENNENT PAS DU PLAY STORE, APP BACKUP & RESTORE POURRA VOUS TIRER D'AFFAIRE...

01 > SAUVEGARDEZ LES APPLICATIONS

Si elle ne l'est pas déjà, insérez votre carte SD dans votre tablette.

Lancez ensuite

App Backup & Restore pour

afficher la liste des applications installées sur l'appareil.

Sélectionnez les applications à sauvegarder (ou

sélectionnez-les toutes à l'aide du bouton en bas à droite) et pressez **Sauvegarder**.



Une fois la carte détectée, installez puis lancez **App Backup & Restore**. Celle-ci vous proposera de déplacer les applis archivées dans le répertoire de sauvegarde.

03 > RESTAUREZ LES APPLICATIONS (AVEC SD)

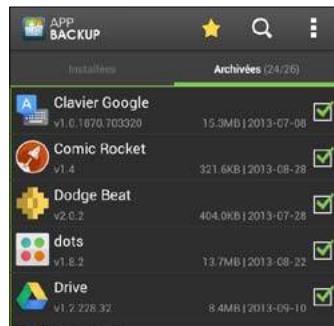
Rendez-vous à présent dans l'onglet **Archivées** où vous retrouverez toutes les applications de votre ancien téléphone. Une fois encore, sélectionnez-les toutes, et touchez le bouton **Restaurer**. Les applications vont alors s'installer une par une, et il vous faudra pour chacune d'elle presser **Installer**, puis **OK**.

02 > PRÉPAREZ LE NOUVEL APPAREIL

Insérez maintenant la carte Micro-SD dans votre nouvel appareil, et en attendant que celle-ci soit détectée, rendez-vous dans



Paramètres > Sécurité et cochez **Autoriser l'installation en provenance de sources inconnues**.



La solution de sauvegarde idéale pour les bidouilleurs qui ne passent pas forcément par le Google Play Store



Certaines préférences ne sont pas enregistrées



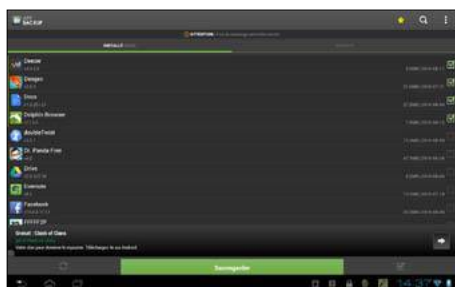
APP BACKUP & RESTORE (SANS CARTE SD)

PRATIQUE



01 > SAUVEGARDER SUR GOOGLE DRIVE

Si l'un ou l'autre de vos appareils ne dispose pas de port SD, pas de soucis, on peut faire autrement. C'est juste un peu plus long. Sauvegardez vos



applications comme indiqué page précédente, puis rendez-vous dans l'onglet **Archivé**. Il vous faudra alors faire un appui long sur chaque appli, touchez **Envoyer**, puis **Drive**.

02 > PRÉPAREZ LE NOUVEL APPAREIL

Là encore, il vous faudra autoriser l'installation en provenance de sources inconnues. Ouvrez donc les **Paramètres** du nouvel appareil, et dans **Sécurité**, cochez **Autoriser l'installation en provenance**



de sources inconnues. S'il n'est pas déjà présent, installez aussi Google Drive et connectez-vous à votre compte Google.

03 > RESTAURER DEPUIS GOOGLE DRIVE

Pour restaurer vos applications sur le second appareil, même plus besoin d'App Backup & Restore. Ouvrez simplement votre Google Drive et retrouvez-y les applications que vous y avez importées. Touchez le fichier pour l'ouvrir, et sélectionnez **Vérifier et installer**. Dans quelques instants, l'application sera installée sur votre appareil.



RÉCUPÉRER SES APPLIS DEPUIS LE PLAY STORE

Pour retrouver toutes les applications que vous avez un jour installées depuis le Play Store, ouvrez l'application Google Play Store et depuis le panneau latéral sélectionnez **Mes Applications**. Trouvez maintenant les applications que vous désirez récupérer, et cliquez sur **Installer**. Tout se passera alors comme n'importe quelle installation du Play Store sauf que vous n'aurez évidemment pas besoin de repayer.





PROTÉGER VOS APPLICATIONS DES REGARDS INDISCRETS

AppLock va
BLOQUER L'ACCÈS À
CERTAINES FONCTIONS
OU APPLICATIONS
AUX PERSONNES NON
AUTORISÉES. SI VOUS
PRÊTEZ VOTRE TABLETTE
À UN ENFANT OU UN AMI,
IL NE POURRA PAS OUVRIR
VOS SMS, PHOTOS OU
VOTRE COMPTE PayPal
PAR EXEMPLE...

01 > LE CODE

Après l'installation, l'appli vous demandera de saisir un code d'au moins 4 chiffres qui servira à débloquent les applications que vous aurez choisies. Retapez ce code et validez. Vous pourrez aussi entrer un e-mail de sécurité, avant d'être dirigé vers la page principale.



02 > LES APPLIS BLOQUÉES

Ici, vous pourrez choisir les applications que vous voudrez bloquer :

photos, vidéos, Google Play Store, paramètres, Facebook ou toutes celles que vous aurez téléchargées. Il suffit de cliquer sur le cadenas. La prochaine fois que vous voudrez la lancer, il faudra saisir votre code.



Parfait pour éviter les yeux indiscrets de votre petite amie ou les gros doigts de votre neveu



Pour chipoter, il ne s'agit pas d'une vraie solution de chiffrement

03 > CRÉER UN PROFIL

Vous pouvez configurer un profil avec accès à certaines applications et pas d'autres, pour prêter votre tablette sans risque. Toucher les 3 lignes parallèles en haut à gauche puis **Profils** et **Invité** (ou le « + » pour en faire un nouveau). Verrouillez/déverrouillez les applis comme à l'étape et validez.



TÉLÉCHARGER // STREAMING MAGAZINE INTERDIT



CHEZ VOTRE MARCHAND DE JOURNAUX !



CHIFFREZ vos SMS FACILEMENT !



La seule option pour chiffrer des SMS sur le réseau GSM. Pratique quand vous n'avez pas moyen de vous connecter à Internet...



Comme d'habitude avec ce genre de système il faudra que vos correspondants utilisent aussi SMSSecure pour que le chiffrement soit actif

PAS ENVIE DE VOUS FAIRE INTERCEPTER VOS SMS PAR DES PETITS CURIEUX ASSIS DANS UN BUREAU À WASHINGTON OU À PARIS ? POUR CHIFFRER COMPLÈTEMENT VOS TEXTOS OU MMS, LA NOUVELLE SOLUTION S'APPELLE SMSSECURE. CETTE APPLI INTERDIT AUSSI LA LECTURE DE VOS MESSAGES EN LOCAL AUX PERSONNES NON AUTORISÉES.

En mars de cette année, les responsables de l'appli TextSecure (voir encadré) ont annoncé que leur bébé ne supportera plus le chiffrement des SMS. En effet,

depuis la version 2.7, cette appli permet toujours de chiffrer des messages, mais sans passer par le protocole GSM. Pour envoyer des messages chiffrés il faut donc utiliser le WiFi ou la 3G un peu



PROTECTION

Textos & MMS

à la manière de Whatsapp (qui intègre Axolotl le protocole de TextSecure). Du mécontentement de nombreux utilisateurs est né un «fork» de TextSecure: SMSSecure. Comme son prédécesseur, SMSSecure va s'ajouter à votre appli standard d'envoi de SMS pour vous proposer de chiffrer en 256 bits vos textos ou MMS avant de les envoyer à vos destinataires. Même si un gouvernement ou un pirate arrive à intercepter vos correspondances, les petits curieux n'auront dans les mains qu'une suite de caractères incompréhensible. Pour que cela fonctionne, il faut que SMSSecure soit installé sur les appareils de vos amis. Et ne pensez pas qu'il s'agit d'une appli réservée à ceux

ayant les derniers téléphones: Android 2.3 suffit amplement!

VOS SMS PROTÉGÉS EN LOCAL AUSSI

En local, un pirate qui aurait votre téléphone dans les mains ne pourra accéder à vos messages qu'avec un mot de passe. Les SMS chiffrés ne sont accessibles que depuis l'interface de SMSSecure (alors que sur TextSecure on pouvait voir les messages en version chiffrés dans l'appli SMS standard): le déni est alors possible («Quoi, mais non je te jure, regarde mes SMS!»). Notez que SMSSecure et TextSecure ne sont pas incompatibles. Utilisez SMSSecure pour les SMS et TextSecure (ou Whatsapp) pour les discussions via Internet!

WHATSAPP SE MET AU CHIFFREMENT DE BOUT EN BOUT !



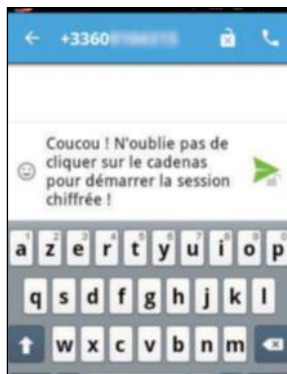
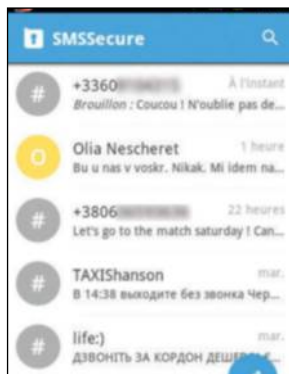
Dans le *Guide de Pirate n°2* nous vous avons parlé de TextSecure une application qui permettait de chiffrer vos messages écrits et MMS sur les réseaux mobiles. Depuis la version 2.7 l'appli se cantonne uniquement à chiffrer des messages via Internet. Sachez d'ailleurs que le code de TextSecure (Axolotl) a été implémenté de base à toutes les versions de WhatsApp. Cette appli devient donc le premier service de messagerie grand public à intégrer du chiffrement de bout en bout... La cerise sur le gâteau c'est que Whatsapp est disponible sur presque toutes les plates-formes mobiles: Android, iOS, Symbian, Windows Mobile Nokia S40 et BlackBerry.





COMMENT FONCTIONNE SMSSECURE ?

PRATIQUE



01 > PREMIERS PAS

Dès le premier lancement, l'appli vous demandera si vous désirez importer vos SMS existants. Pas de panique il s'agit de vous faciliter vos communications, rien ne bougera dans votre appli SMS standard. Choisissez un correspondant et envoyez-lui un message. Si cette personne ne possède pas encore SMSSecure, elle sera invitée à le télécharger. Attention, à ce stade, les SMS ne seront pas chiffrés!

TÉLÉPHONEZ CHIFFRÉ AVEC DISCRETIO



Dans le *Guide de Pirate n°1* nous vous avons présenté Discretio, une appli révolutionnaire qui permet à deux correspondants de communiquer en WiFi ou 3G. L'authentification comme le contenu de la conversation seront chiffrés et même une analyse poussée des paquets ne révélera rien. Si vous souhaitez vous la jouer Jack Bauer ou tout simplement éviter les IMSI Catcher (voir page 58)...

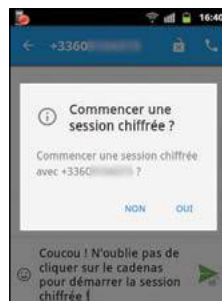
Lien : www.discretio.com



DISCRETIO

02 > UN ÉCHANGE DE CLÉ TRANSPARENT

Lorsque votre correspondant aura installé l'appli, il pourra passer par cette dernière pour vous répondre. L'échange de clés de chiffrement est transparent pour vous: rien à gérer de ce côté, vous verrez juste une petite clé dans un message! Vous pourrez alors commencer une session chiffrée en cliquant sur le cadenas en haut. Le cadenas fermé à droite à côté de la flèche d'envoi montre que votre session est chiffrée. Ni les services secrets, ni la police, ni l'opérateur ne pourront déchiffrer votre conversation.



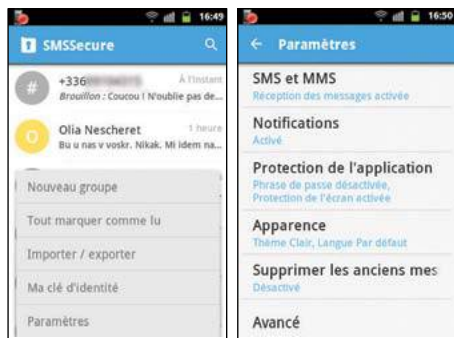


PROTECTION

Textos & MMS

03 > LES OPTIONS

Dans la liste globale des SMS, il est possible d'appuyer sur le bouton menu du téléphone pour avoir accès à certaines options. Vous pouvez par exemple faire des groupes de correspondants, **Importer/Exporter** des messages depuis et vers SMSecure ou avoir accès à votre clé publique. Dans **Paramètres** vous pourrez effacer les anciens messages automatiquement après une durée déterminée, mais nous vous conseillons avant tout d'aller dans **Protection** de l'application.



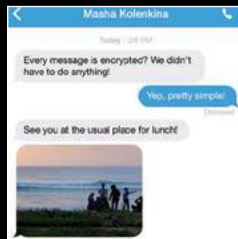
ET SUR IOS ?



Sur iOS, foin de SMSsecure, mais une autre application intéressante :

Signal. Cette dernière permet d'envoyer des messages chiffrés de bout en bout avec l'application TextSecure, sous Android ! Des utilisateurs de Signal peuvent donc communiquer de manière sécurisée entre eux ainsi qu'avec les utilisateurs de TextSecure sur le système concurrent... Les vidéos et photos sont aussi de la partie. Par contre pas de chiffrement pour les SMS via le réseau GSM.

Lien : <https://goo.gl/TQwh27>

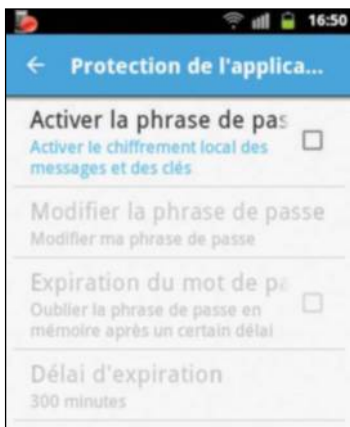


04 > PROTECTION EN LOCAL

Pour protéger en local vos SMS (dans le cas d'un vol... ou d'une petite amie jalouse) il faudra cocher la case **Activer**

la phrase de passe.

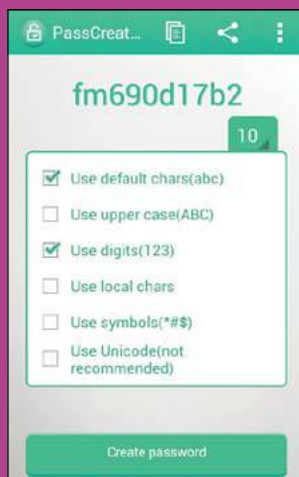
Ici vous pourrez aussi paramétrer un délai d'expiration pour ce sésame. Choisissez un mot de passe solide, mais prenez garde : il ne faudrait pas l'oublier ! La prochaine fois que vous voudrez accéder à SMSsecure, ce mot de passe vous sera demandé.





DES MOTS DE PASSE SUR MESURE

// AVEC MOT DE PASSE GÉNÉRATEUR



Vous avez du mal à trouver des mots de passe «solides»? Mot de passe générateur le fait pour vous. Il vous suffit de sélectionner le nombre de caractères dont vous avez besoin (entrel et 256) et le tour est joué. L'application choisit chaque lettre de manière complètement aléatoire, ce qui renforce considérablement la «force» du précieux sésame puisqu'il n'a aucune signification. Attention toutefois, le résultat peut être difficile à retenir. Pour iOS il existe l'appli Sécurité Maxium : <https://goo.gl/Cm9GTG>.



<https://goo.gl/crXC4Y>

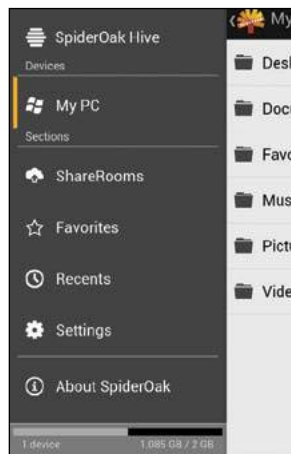
UN CLOUD CRYPTÉ

// AVEC SPIDER OAK

Nous vous avons déjà parlé de BoxCryptor dans ce numéro, mais si vous cherchez une alternative, pourquoi ne pas essayer Spider Oak? Le service coûte 10dollars pour 100Go de stockage, mais vous pouvez opter pour l'offre gratuite avec 2Go. Bien sûr, il existe des versions pour Android, iOS, mais aussi Windows, MacOS et Linux. Sachez enfin que le chiffrement est un mélange entre RSA 2048bits et AES 256bits et que tout se fait en local. Impossible pour un pirate de récupérer la clé donc...



<https://spideroak.com>



UN VPN GRATUIT

// AVEC SECURITYKISS



SecurityKISS est un VPN compatible avec les deux principaux protocoles OpenVPN et PPTP. Très pratique pour changer de localisation et tunneler sa connexion, ce type de service s'adresse surtout aux utilisateurs qui souhaitent protéger leurs appareils des pirates lorsqu'ils se connectent à des réseaux WiFi peu sûrs. SecurityKISS est gratuit, mais limité à 300Mo de trafic par jour (tranche de 24heures)...



www.securitykiss.com



VÉRIFIEZ QUE CE TÉLÉPHONE N'A PAS ÉTÉ VOLÉ

// AVEC CHEEK CHECK



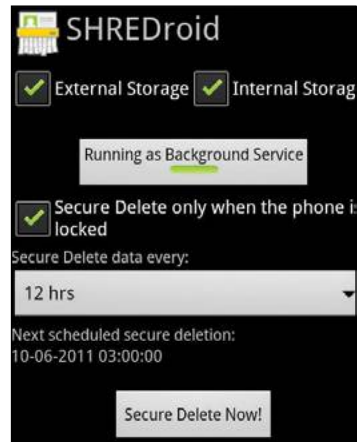
Vous allez acheter un téléphone d'occasion, mais vous avez des doutes sur le vendeur ? Avec le site Cheek Check vous allez pouvoir être sûr que l'appareil n'a pas été volé ! L'astuce fonctionne sur tous les téléphones et quelque soit l'opérateur, car il s'agit de vérifier si le numéro IMEI du téléphone n'est pas dans la base de données mondiale des téléphones volés ou perdus. Allez sur le site et sur la droite choisissez le français. Entrez le code IMEI dans le champ et cliquez sur **Vérifier**. Pour avoir ce code il suffit de taper ***#06#** sur l'appareil en question. Notez qu'il est possible d'utiliser une application Android pour vérifier discrètement sur un autre téléphone au moment de l'achat.

www.cheek-check.com



EFFACEZ VOS TRACES

// AVEC SHREDROID



SHREDroid est une application qui permet d'effacer toutes traces des fichiers que vous voulez voir disparaître. Il est en effet possible pour un pirate de récupérer des fichiers partiellement effacés sur votre mémoire interne ou carte SD. L'appli va enregistrer des données aléatoires là où étaient stockés vos fichiers pour être sûr de ne rien laisser de compromettant.

<https://goo.gl/UZ5Dx6>

GÉREZ VOTRE MONNAIE VIRTUELLE

// AVEC BITCOIN WALLET



Vous utilisez les Bitcoins pour payer vos achats sur Internet ? Bitcoin Wallet va vous permettre de gérer tous les aspects de cette monnaie virtuelle: conversion en devises, affichage des montants paramétrable (BTC, mBTC ou µBTC), réception d'argent ou paiement via Bluetooth, NFC, QR Code, etc. L'application n'est pas rattachée à un site et fonctionne de manière complètement autonome.

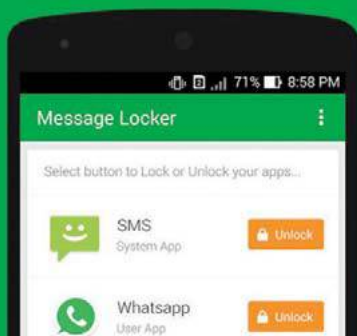
<https://goo.gl/CsIs6v>

Unit	Rate	Balance
USD (default)	rate: 327952.50	balance: 112.44
UYU	rate: 6.17	balance: 2944.04
UZS	rate: 993.90	balance: 28322.42
VBF	rate: 1.50	balance: 713.44
VND	rate: 5112.73	balance: 2439059.32
VUV	rate: 25.04	balance: 11945.69

Date	Transaction	Amount
Apr 30	1CQh RCTg cRKA BPFB xDeV vNNA rFnJ...	-4.20
Apr 22	1Nob NwC3 9H9r adV9 N9w d9p9 mm...	-21.29
Apr 17	18CK 5K1g aJRK KSC7 yVST XT9L Ez9h...	+13.09
Apr 17	18CK 5K1g aJRK KSC7 yVST XT9L Ez9h...	+1.00



Verrouillez toutes vos applications de messagerie dans juste un robinet.



VERROUILLEZ VOS SMS



// AVEC MESSAGE LOCKER

180 milliards. C'est le nombre de SMS envoyé en France chaque année. Alors forcément, certains de vos messages contiennent des informations sur votre vie privée que vous ne souhaitez sûrement pas révéler au premier venu. Message Locker vous permet de bloquer l'accès à toutes vos applications de messagerie, de mail et même à certains de vos réseaux sociaux avec un code PIN. Simple et très efficace.



<https://goo.gl/dApc7G>

ÉVITEZ LES MESSAGES ALCOOLISÉS

// AVEC DRUNK LOCK



Parfois, il faut savoir se protéger de soi-même. Pour éviter d'envoyer des textos bourrés à votre ex, installez donc l'application Drunk Lock. Ouvrez simplement l'appli pour activer le blocage, et vous ne pourrez ni appeler ni envoyer de messages avant d'avoir répondu à trois questions mathématiques.

Le niveau des questions est paramétrable, mais attention, elles seront en anglais. Pour les appareils Apple, il existe Drunk Text Savior : <https://goo.gl/A5hTDG>.



<https://goo.gl/b5QQPp>



DES DOCUMENTS QUI S'AUTODÉTRUISENT



// AVEC DIGIFY



Voici un petit logiciel directement inspiré de la série Mission Impossible. Digify permet de mettre un fichier à disposition pour un ou plusieurs correspondants, mais seulement pendant une durée limitée (de une minute à un mois). Au bout de ce délai, votre fichier «s'auto-détruit». Il faudra juste que les utilisateurs s'inscrivent pour utiliser Digify. Les utilisateurs de Dropbox pourront aller chercher directement les documents dans leur Cloud et vous pourrez même être averti si un de vos correspondants prend une capture d'écran.



www.digify.com



UN DÉVERROUILLAGE MALIN

// AVEC SMART UNLOCK

Verrouiller son téléphone, c'est important, mais entrer son code à chaque fois, c'est aussi fatigant. Smart Unlock permet ainsi de déverrouiller automatiquement son téléphone lorsqu'il est connecté à votre Wi-Fi ou à proximité d'un de vos appareils Bluetooth. Lorsque vous serez chez vous, vous n'aurez donc plus à saisir le schéma de déblocage.



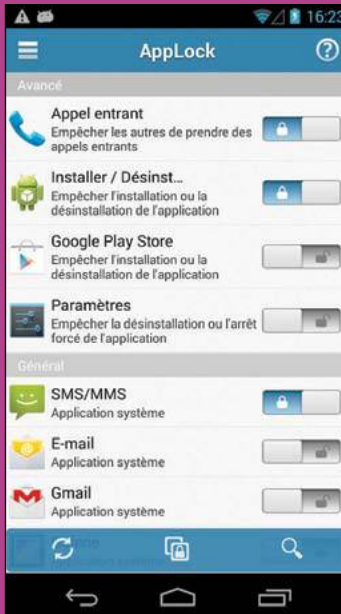
<https://goo.gl/y7UNcA>



VERROUILLEZ VOS APPLIS

// AVEC SERRURE (AppLock)

Voilà une application bien nommée! Serrure permet de protéger n'importe quelle fonctionnalité/application de votre téléphone par un même mot de passe. Pratique, si vous prêtez souvent votre smartphone et souhaitez éviter les mauvaises surprises. Évidemment, vous n'aurez pas besoin d'entrer ce mot de passe vous-même, à chaque fois, il vous suffira d'ouvrir l'application (elle aussi protégée par mot de passe) pour activer ou désactiver l'AppLock. Par ailleurs, Serrure vous permettra aussi de cacher aux yeux de tous d'éventuelles photos et vidéos compromettantes.

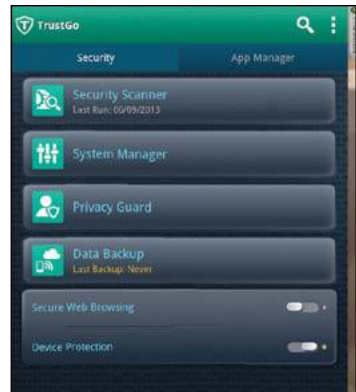


<https://goo.gl/yDVnQb>



UN ANTIVIRUS PERFORMANT

// AVEC TRUSTGO ANTIVIRUS



TrustGo est l'un des meilleurs antivirus disponibles sur Android: en plus de fournir une très bonne protection contre les malwares, l'application embarque de nombreuses fonctions. De la gestion de la mémoire vive à la sauvegarde de vos données dans un Cloud en passant par un système antivol qui vous envoie la photo de la personne qui essaye de forcer votre mot de passe, TrustGo est un must have en matière de sécurité.



www.trustgo.com



NOUVEAU !

**INSCRIVEZ-VOUS
GRATUITEMENT !**

Le mailing-list officielle de *Pirate Informatique* et des *Dossiers du Pirate*

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la « Commission paritaire des publications et agences de presse » (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner
directement sur ce site

<http://eepurl.com/FLOOD>

(le L de « FLOOD » est en minuscule)

ou de scanner ce QR Code avec
votre smartphone...



TROIS BONNES RAISONS DE S'INSCRIRE :

- 1 Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
- 2 Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
- 3 Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.



MULTIMÉDIA



86

μTORRENT pour télécharger sur mobile

88

Le Netflix du pauvre : **POPCORN TIME**

92

SOUS-TITRES sur mobile : Nos solutions



INFOS [µTorrent]

Où le trouver ? [<https://goo.gl/0vF3HB>]

Difficulté :

TÉLÉCHARGER AVEC µTORRENT

POUR REGARDER DES FILMS
ET DES SÉRIES SUR
VOTRE APPAREIL MOBILE,
VOUS TÉLÉCHARGEZ VIA
TORRENT AVANT DE
TRANSFÉRER LES
FICHIERS ? NOUS AUSSI !
ENFIN C'EST CE QUE
NOUS FAISONS AVANT
QUE µTORRENT SE DOTE
D'UNE VERSION ANDROID
QUI PERMET DE TOUT FAIRE
DEPUIS VOTRE TABLETTE/
SMARTPHONE...



Téléchargez ses .torrent depuis son PC pour profiter des fichiers depuis son cloud ou son NAS c'est tellement «2014». Avec µTorrent sur Android vous pouvez télécharger directement vos fichiers sur votre mobile pour en profiter localement. Il faudra bien sûr disposer d'assez d'espace de stockage sur votre mobile ou votre carte SD, mais cette solution convient particulièrement bien aux utilisateurs nomades. Téléchargez une vidéo dans la journée (en WiFi ou 3G) pour en profiter le soir à l'hôtel, au camping ou dans l'avion.

VOUS NE SEREZ PAS DÉPAYSÉS

Pas de client, de téléchargement ou de ratio à gérer ici. Il suffit de choisir son film dans l'interface principale ou de le trouver par mot clé. Au bout de quelques secondes, la vidéo s'active et vous pouvez même

avancer pour passer un générique sans faire bugger le tout. Pour ce genre d'utilisation, le .torrent doit être en bonne santé. Il faut en effet que beaucoup de personnes soient en train de le visionner ou de le «seeder» pour que le film ne saccade pas. Dans Popcorn Time, ce sont les administrateurs qui sélectionnent les .torrent pour vous, retirent ceux en mauvaise santé et les remplacent. Pour l'utilisateur, toute la partie «pénible» est donc supprimée. En ce qui concerne les films, il s'agit de blockbusters américains ou de films à succès. La plupart du temps, vous pourrez choisir la qualité (720 ou 1080p) et élément indispensable pour les non-anglophones, les sous-titres. Plus de la moitié des films présents intègrent des sous-titres en français et tous ont au moins des sous-titres anglais. Idéal pour se faire une séance ciné à la maison lorsqu'on n'a rien à se mettre sous la dent...



Téléchargez directement de votre appareil mobile sans passer par un ordinateur



Deux options payantes qui auraient pu être gratuites

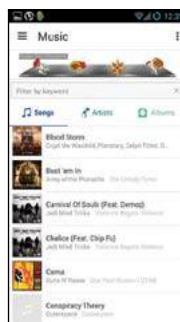
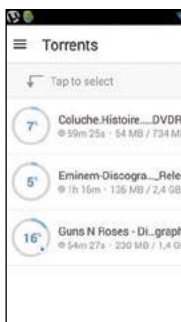
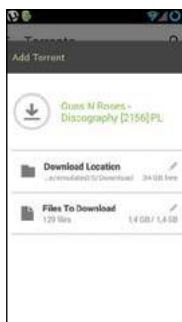
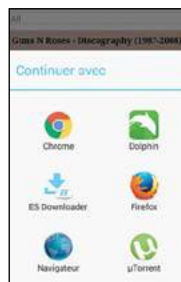


CHERCHER, TROUVEZ ET TÉLÉCHARGEZ !

PRATIQUE

01 > PREMIERS PAS

Une fois l'application installée, il suffira de chercher un fichier Torrent depuis le moteur de recherche (la loupe en haut à droite). Rien de bien sorcier, l'appli ira demander à Google. Attention pour certains trackers, il faudra être inscrit ! Utiliser le navigateur et cliquer sur le Torrent ou le lien magnet. Demandez ensuite à µTorrent de prendre la relève.

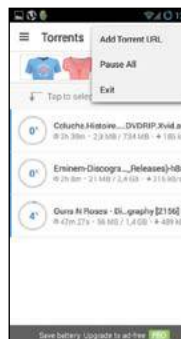
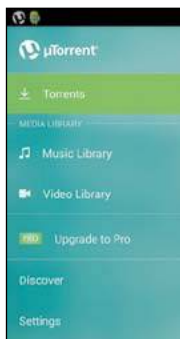


02 > L'INTERFACE

L'appli vous indiquera alors où sera stocké le fichier final puis il ira rejoindre les téléchargements en cours dans l'interface. Il est possible de sélectionner les différents Torrents pour en explorer le contenu. Une fois téléchargés les fichiers seront automatiquement intégrés aux bibliothèques. Les autres contenus multimédias s'y retrouveront aussi.

03 > LES OPTIONS

En haut à gauche vous aurez accès à un menu vous donnant l'accès aux bibliothèques, mais aussi aux paramètres (Settings). Notons ici que deux options manquent à l'appel: la possibilité d'économiser la batterie et d'éteindre automatiquement l'appli lorsqu'elle n'est pas utilisée. Il faudra payer 3 € et passer à la version Pro pour y avoir accès... Pour ajouter un Torrent à la main, il faudra appuyer sur les trois petits points en haut à droite.





INFOS [POPCORN TIME]

Où le trouver ? [<http://popcorn-time.se>]

Difficulté : 



POPCORN TIME : L'ALLIANCE DU STREAM ET DU P2P

DIFFICILE DE CHOISIR ENTRE LE STREAM ET BitTorrent. LE PREMIER PROPOSE L'IMMÉDIATÉTÉ TANDIS QUE LE SECOND PROPOSE DU CONTENU DE QUALITÉ. POPCORN TIME ALLIE POURTANT LES DEUX EN PERMETTANT DE VOIR IMMÉDIATEMENT UN FILM À PARTIR DE BitTorrent. ET MÊME PAS BESOIN DE CHERCHER DES FICHIERS COMPATIBLES PUISQUE VOUS N'AVEZ QU'À CLIQUER DANS LA LISTE ET FAIRE CHAUFFER LE POPCORN...



Popcorn Time a fait son apparition sur Internet au printemps dernier. La nouvelle d'un logiciel permettant un visionnage de qualité, immédiat, sans pub, avec un moteur de recherche intégré a fait tellement de bruit que les auteurs ont préféré arrêter le développement. Peur des représailles des ayants droit ? Différend philosophique entre eux et leurs utilisateurs ? On ne

saura jamais. Toujours est-il que sa réputation de «Netflix pour pirates» s'est répandue comme une traînée de poudre et que de nombreux logiciels ont pris la relève.

COMMENT ÇA MARCHE ?

Pas de client, de téléchargement ou de ratio à gérer ici. Il suffit de choisir son film dans l'interface principale ou de le trouver par mot clé. Au bout de quelques



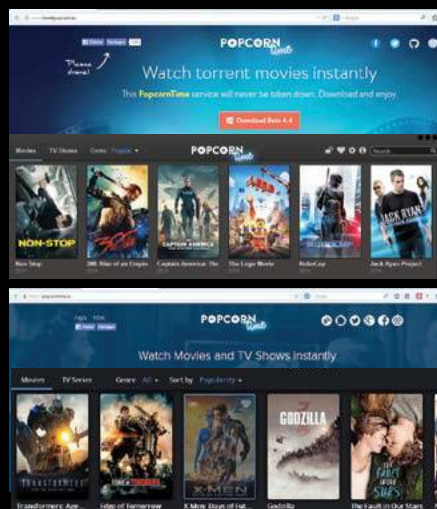
Des vidéos récentes, à la demande et sans pub.



Donne accès à du contenu essentiellement illégal

UN LOGICIEL, DEUX VERSIONS

Difficile de différencier ces deux «forks» nés du Popcorn Time original. Et pour cause : ces deux logiciels reprennent à la fois le nom et le logo de l'illustre prédécesseur. Le premier sur <http://popcorn-time.se> et le second à l'adresse <https://popcorntime.io>. Les sites et les interfaces des logiciels se ressemblent énormément. Il est même très difficile de les différencier. Sachez juste que sous Windows les deux se valent au niveau de contenu vidéo et des sous-titres. De même les deux proposent des applications pour Android 4.0 (à télécharger sur leurs sites respectifs et pas sur le Play Store). Pour les machines Apple, seule la version en .se propose une compatibilité avec les appareils «jailbreakés». Les deux proposent aussi une connexion via VPN pour contourner la surveillance même si selon Numerama, il est question de basculer sur le protocole i2P pour le .se. Seule différence au niveau technique, l'absence d'un mode lecture hors connexion sur le .io. Côté



contenu, vous ne trouverez que des grands succès, des blockbusters et des séries TV qui ont pignon sur rue. La popularité des .torrent est primordiale pour afficher rapidement la vidéo. Les fans d'animés japonais se tourneront en priorité vers Popcorn Time.io



INFOS [POPCORN TIME]

Où le trouver ? [<http://popcorn-time.se>]

Difficulté : 

secondes, la vidéo s'active et vous pouvez même avancer pour passer un générique sans faire bugger le tout. Pour ce genre d'utilisation, le fichier .torrent doit être en «bonne santé». Il faut en effet que beaucoup de personnes soient en train de le visionner ou

de le «seeder» pour que la vidéo ne saccade pas. Les administrateurs de ces logiciels doivent donc mettre souvent à jour les fichiers. C'est toujours ça en moins à faire pour vous ! Notez qu'il est souvent possible de choisir la qualité et d'afficher des sous-titres.



UNE SORTE DE NETFLIX GRATUIT AVEC UN CHOIX DITHYRAMBIQUE !

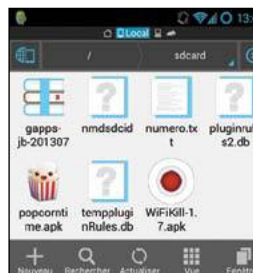
PRATIQUE



POPCORN TIME SUR MOBILE

01 > LE FICHIER D'INSTALLATION

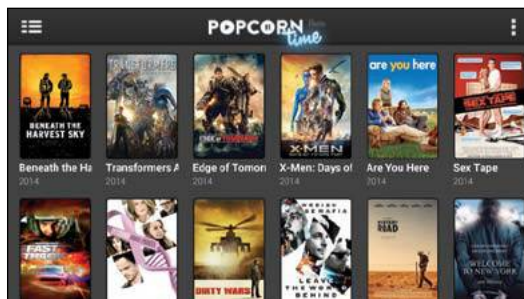
Nous verrons ici comment installer la version Android mais sachez que Popcorn-time.se propose aussi une version pour iPhone et iPad. Il vous faudra néanmoins un appareil «jailbreaké» pour en profiter (voir page 10). Commencez par télécharger le fichier APK depuis le site en déroulant la page principale vers le bas. Attention, l'appli ne fonctionnera que sur des appareils ayant au moins une version 4.0 d'Android. Transférez ensuite ce fichier .apk avec un câble USB ou en vous l'auto-envoyant par e-mail depuis un PC.



02 > L'INTERFACE

Lancez alors ce fichier APK (avec votre gestionnaire de fichiers) et n'oubliez pas d'autoriser l'installation d'applications issue d'une autre source que du Play Store (**Paramètres > Sécurité > Sources Inconnues**). Dès que l'installation sera terminée, vous retrouverez la même interface claire et

conviviale de la version PC. En haut à gauche, vous pourrez choisir entre les films et les séries tandis que les paramètres s'afficheront depuis le menu à droite.



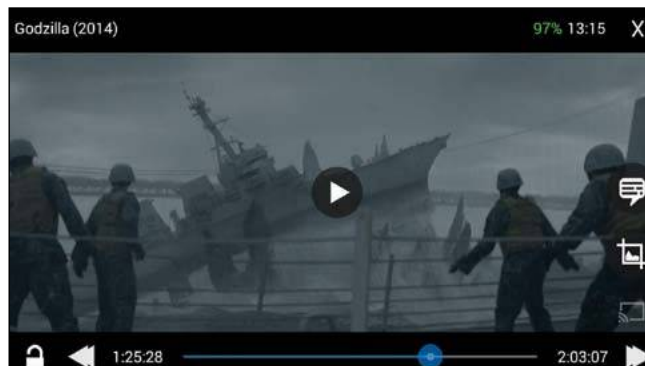


03 > LE CHOIX

Après avoir choisi votre vidéo, vous aurez ici aussi le loisir de sélectionner vous-même votre Torrent: qualité, codec, bitrate, etc. Faites **Watch it Now** et attendez que le film se mette en cache (dans la racine de la mémoire interne à **storage/emulated/0/time4popcorn**). Les paramètres

(Settings)

permettront de changer la langue de l'interface, d'activer le VPN, accélération matérielle et les sous-titres sélectionnés par défaut.



04 > C'EST TOUT!

Lorsque la lecture aura démarré, vous pourrez choisir une autre piste de sous-titres, changer le ratio de l'image (4/3, 16/9, etc.) et verrouiller l'écran tactile pour éviter les erreurs de manipulation pendant la lecture. Dès que vous aurez fini vos réglages, le player se mettra automatiquement en plein écran bien sûr.





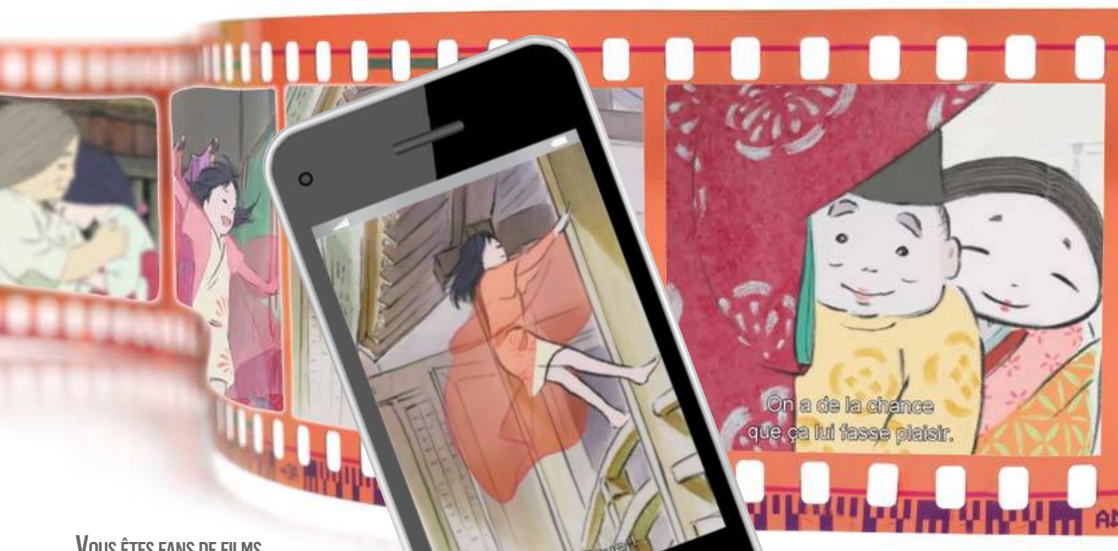
INFOS [MX PLAYER] Où le trouver ? [<https://goo.gl/fmt4Lm>]

[GMT SUBTITLES] Où le trouver ? [<http://goo.gl/Vjtlhz>]

[SUBTITLESFINDER] Où le trouver ? [<http://goo.gl/rVbrYi>]

Difficulté: ☠☠☠

LES SOUS-TITRES SUR MOBILES



VOUS ÊTES FANS DE FILMS
OU SÉRIES TV EN VO ?
BIEN SÛR VOUS SAVEZ
BIEN COMMENT GÉRER LES
FORMATS DE FICHIERS SUR
PC OU MEDIA CENTER,
MAIS SAVIEZ-VOUS QUE VOTRE
APPAREIL MOBILE EN EST
AUSSI CAPABLE ? VOYONS
LES DIFFÉRENTES SOLUTIONS
QUI S'OFFRENT À VOUS POUR
TROUVER DES SOUS-TITRES ET
LES AFFICHER...

Les sous-titres que vous pouvez trouver sur le Net sont soit des captures de caractères récupérés sur des DVD ou des Blu-ray, soit des fichiers spécialement créés par des équipes de fans appelés fansubbers. Dans les deux cas, si s'agit de fichiers textes qui doivent être lus par votre logiciel

de lecture en même temps que la vidéo. Parfois il suffit de cocher une case dans votre appli de lecture multimédia (lorsque le texte est intégré au fichier vidéo), mais parfois il faudra trouver et faire afficher le fichier .sub, .srt, .ssa ou .txt pour profiter d'un film chinois ou d'une série américaine.



TROUVER ET AFFICHER VOS SOUS-TITRES

PRATIQUE

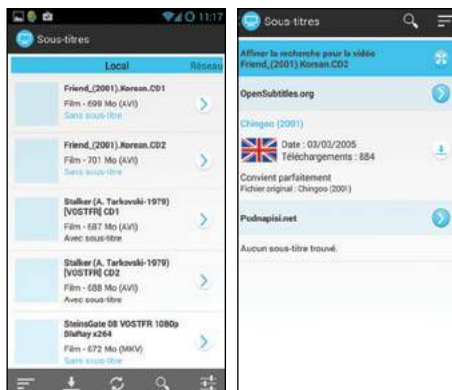


01 > MX PLAYER POUR ANDROID

Pour lire vos fichiers multimédias avec sous-titres, rien ne vaut MX Player. Ce lecteur compatible la plupart des formats de fichiers est aussi à l'aise avec les sous-titres encapsulés qu'avec ceux aux formats SUB, SRT, SSA ou TXT. Il suffit de cliquer dans la bulle de texte en haut à droite pour choisir sa langue. Le choix de la piste sonore (quand il y en a plusieurs) est aussi de la partie.



02 > CHERCHER DES SOUS-TITRES



Vous avez le fichier vidéo, mais pas le sous-titre qui va avec ? Pas de problème avec GMT Subtitles !

L'appli va scanner les fichiers multimédias présents sur votre machine et vous proposer des sous-titres adéquats. Les fichiers texte seront placés « à côté » de votre vidéo pour lancer les deux avec MX Player.



03 > ET POUR LES PRODUITS APPLE ?

Pour les iPhone/iPad c'est un peu plus compliqué (comme toujours avec ces systèmes fermés !). Il faudra d'abord installer un lecteur compatible avec les formats de vidéos et de sous-titres les plus courants (par défaut, l'iPad ne lit en effet que les fichiers MP4). Ensuite, il faudra se tourner vers l'appli SubtitleFinder, disponible sur iTunes pour 0,99€. Son fonctionnement est un peu différent : l'application va chercher, renommer et placer les sous-titres des vidéos présentes sur votre box ou lecteur de salon, du moment qu'ils sont accessibles par FTP ou Samba. Vous devrez ensuite transférer le tout sur votre appareil Apple.

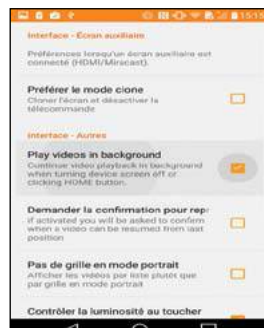




UNE VIDÉO EN ARRIÈRE-PLAN

// AVEC VC MEDIA PLAYER

Dans VLC, cliquez sur les trois barres horizontales en haut à gauche pour ouvrir le menu contextuel, allez ensuite dans **Préférences** puis **Interface** sous **Réglages supplémentaires**. Il vous suffit désormais de cocher **Play videos in background** et l'option sera alors activée et vos vidéos continueront leur lecture même après avoir minimisé VLC. Ensuite, dans le menu contextuel, vous pouvez choisir **Vidéo**, l'application listera alors tous les fichiers vidéo disponibles sur votre appareil, ou vous pouvez aller dans **Dossiers** pour rechercher une vidéo spécifique manuellement. Pour minimiser l'application, vous pouvez simplement appuyer sur votre bouton **Home** et la vidéo continuera de tourner en arrière-plan. L'intérêt principal de cette fonctionnalité est tout simplement la fluidité de lecture. Si vous recevez par exemple un SMS ou un e-mail que vous souhaitez consulter, la lecture en arrière-plan vous permettra de ne pas interrompre totalement votre activité.



 <https://goo.gl/6kyRZw>

ADAPTER LA RÉOLUTION

// AVEC SECONDSCREEN

Cette appli va vous changer la vie si vous avez l'habitude d'utiliser un autre moniteur pour afficher les photos ou vidéos que vous avez sur votre appareil mobile. SecondScreen adaptera la résolution pour avoir la meilleure expérience possible sur votre téléviseur que vous utilisiez Chromecast, un autre système de partage de flux ou simplement votre câble HDMI. Transformez votre appareil Android en console de jeux, PC de remplacement ou disque dur multimédia !



 <http://goo.gl/wDrKe7>



UN CLOUD À LA MAISON

// AVEC BITTORRENT SYNC



BitTorrent Sync propose une alternative amusante au cloud : vos fichiers ne sont pas sur un serveur, mais bien sur votre PC. Une clé unique permet à vos amis d'y avoir accès... Comme le système est décentralisé, la seule limite est celle de la taille de votre disque dur. Grâce à la technologie P2P de BitTorrent, vous synchronisez un ou plusieurs dossiers avec vos amis en leur communiquant une clé secrète unique. Vos amis n'auront qu'à installer le programme et taper votre clé. C'est aussi un très bon moyen pour avoir accès à tous vos fichiers depuis tous vos appareils. Car BitTorrent Sync est disponible Android et iOS mais aussi pour Windows, MacOS, Windows mobile, etc. Le seul défaut par rapport à un serveur cloud c'est qu'il faudra que votre ordinateur soit allumé pour que vos contacts aient accès aux dossiers.



 www.vodkaster.com



DES MATCHS EN DIRECT

// AVEC SOPCAST



Vous avez peut-être déjà expérimenté les retransmissions sportives en direct sur PC avec le logiciel chinois Sopcast. Ici c'est la même chose sauf que ça se passe sur votre mobile ou tablette Android. Il faudra juste chercher des liens compatibles, car la liste des chaînes n'est pas vraiment mise à jour. Contrairement à un stream "normal", plus vous êtes nombreux et meilleure sera la qualité ! Pour trouver des liens **sop://**, vous pouvez toujours commencer par chercher ici : <http://livetv.sx/fr>.



www.vodkaster.com



ENREGISTREMENT VIDÉO DE L'ÉCRAN

// AVEC TORRENT SCR SCREEN RECORDER



SCR Screen Recorder est une application uniquement disponible pour les appareils rootés permettant d'enregistrer en vidéo ce qui se passe sur votre écran. Vous pourrez donc réaliser vos propres tutoriels ou enregistrer le déroulement d'une partie de jeu vidéo. Notez que l'appli gère l'accélération matérielle des dernières puces Tegra et qu'en version gratuite, les vidéos seront limitées à 3 minutes. Largement de quoi faire un petit tuto explicatif...



<http://goo.gl/Nsb3LU>

LIRE LE FORMAT AC3

// AVEC MX PLAYER



MX Player est notre appli chouchou pour lire la vidéo mais malheureusement elle n'est pas nativement compatible avec l'AC3 et le son DTS. Si vous avez une vidéo au format MP4 ou MKV et que le son ne fonctionne pas, c'est sans doute qu'il s'agit d'un problème avec l'AC3. Suivez notre lien et téléchargez l'archive correspondant à votre chips et vidéo (Tegra3 dans notre exemple). Décompactez-la et placez le fichier dans **storage/emulated/0/Download**. Dans **MX Player**, allez dans le menu aux trois petits points puis **Paramètres>Décodeur>Codec personnalisé**. Chargez le fichier, redémarrez MX Player et l'appli devrait maintenant lire le format AC3 sans problème.



<http://goo.gl/GiZW4j>





DES PHOTOS DISCRÈTES

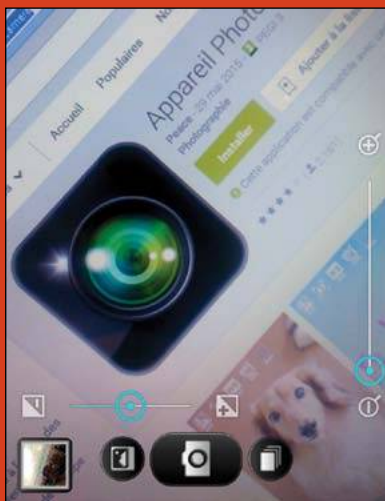
// AVEC APPAREIL PHOTO SILENCIEUX



Vous voulez prendre des photos en toute discrétion? Sans bruits d'obturateur, sans signal sonore et avec la possibilité d'éteindre le flash, cette appli vous permettra de prendre un bébé qui dort, un animal de compagnie ou n'importe quel sujet qui serait alerté par un bruit ou une lumière suspecte. Bien sûr, les principaux réglages d'applis photo standards sont de la partie...



<https://goo.gl/8AIWiW>



PARTAGEZ TOUS VOS FICHIERS MULTIMÉDIAS

// AVEC PLEX



De nos jours, les fichiers multimédias occupent de plus en plus de place sur nos disques durs ou appareils connectés. Le problème c'est que dans un foyer, tous ces fichiers sont éparpillés entre les appareils domestiques: PC, smartphone, tablette ou TV connectée. Plex propose de simplifier les choses pour ses utilisateurs en proposant une solution client/serveur. Il suffit juste de paramétrer un ordinateur (PC ou Mac) en tant que serveur, placer tous vos fichiers sur ce dernier et d'accéder à votre large bibliothèque depuis vos autres appareils en utilisant les applications «clientes». Compatible avec Android et iOS Plex propose une version payante qui permet la lecture hors ligne.



<https://goo.gl/7UwFU>

SYNCHRONISEZ VOS DONNÉES

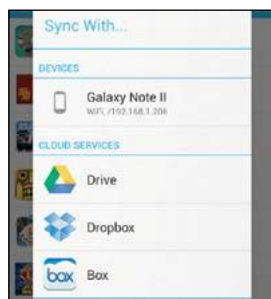
// AVEC DATASYNC



DataSync va vous permettre de synchroniser des données entre différents appareils Android en vous aidant juste de votre connexion Wi-Fi. Vous pourrez donc par exemple récupérer des contacts, des fichiers, des fichiers de sauvegarde, etc. Bien sûr cela fonctionne à merveille pour le multimédia ! Si vous n'avez pas de réseau Wi-Fi dans les environs il est même possible de synchroniser les données à travers un compte Dropbox ou Google Drive en utilisant la 3G...



<http://goo.gl/p4YFHU>





RÉCUPÉREZ VOS FICHIERS EFFACÉS

// AVEC **DISKDIGGER**



DiskDigger permet simplement de retrouver des photos malencontreusement effacées de votre mémoire interne ou de votre carte SD. Qu'il s'agisse d'une erreur de manipulation ou d'un formatage, cette appli va retrouver vos JPEG, PNG ou vidéos MP4 tant que la perte est récente. En effet il faudra agir vite pour que le système n'enregistre aucune information sur les zones où étaient stockés vos précieux fichiers. Le mieux est encore d'installer DiskDigger avant toute tentative de récupération.

    <http://goo.gl/zLY3mC>

PRENEZ DES CAPTURES D'ÉCRAN

// AVEC **SCREENSHOT**



Pour prendre des captures d'écran, vous utilisez le raccourci Volume - / Bouton ON? Mais peut-être avez-vous remarqué que cette astuce ne fonctionne pas tout le temps: impossibilité de l'utiliser dans certaines applications, dans certains menus, etc. Avec un appareil rooté et Screenshot vous n'aurez plus de problèmes! Cette appli permet de prendre des captures dans n'importe quelle circonstance avec un délai, en secouant le téléphone, en inversant certaines couleurs, en forçant la capture, etc.



    <https://goo.gl/nnoVh7>

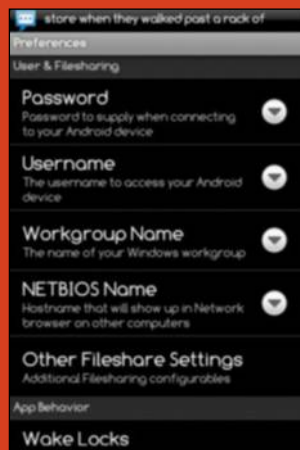
PARTAGER VOTRE CARTE SD VIA WI-FI

// AVEC **SAMBA FILESHARING**

Samba Filesharing est une appli très utile si vous désirez partager le contenu de votre carte SD sur votre réseau domestique. Une fois installée sur votre appareil Android il suffit de retrouver le contenu de votre carte SD avec votre explorateur Windows. Il est même possible de spécifier un mot de passe pour plus de sécurité. Attention, il faudra un appareil rooté pour en profiter!



   <http://goo.gl/jV2NdE>



Matériel

Novodio Multi Fast Charger, UN CHARGEUR RAPIDE, INTERNATIONAL ET POLYVALENT

Avec tous nos appareils mobiles, faire sa valise devient un vrai casse-tête lorsqu'il s'agit de savoir quel chargeur emporter pour quel matériel. Le Novodio Multi Fast Charger propose une solution astucieuse. Non seulement l'appareil permet de recharger 4 machines en même temps, mais elle propose deux



intensités (2x 1A et 2x 2,4A) pour répondre aux différents besoins en énergie. Rien ne vous empêche d'ailleurs de recharger un smartphone nécessitant 1A sur une prise 2,4A. Comme la tension reste au alentour des 5V, votre batterie de risque rien et vous diviserez par deux votre temps de recharge. Cerise sur le gâteau, la prise secteur est interchangeable et 3 autres types de broches sont fournis : Royaume-Uni, USA et Australie (les pays d'Asie ou d'Afrique utilisent forcément un de ces 4 standards).

Prix : **30 €** Lien : <http://goo.gl/jH4luu>

GoTenna, CHÉRIE ÇA VA CAPTER !

GoTenna est une antenne de 14 cm qui se connecte à votre mobile en Bluetooth et qui permet de communiquer avec un correspondant lui aussi équipé même si aucun réseau GSM n'est présent. Si vous habitez ou travaillez dans une zone blanche, cet appareil vous permettra de joindre un ou plusieurs camarades sans frais et sans passer par un satellite ! La zone de couverture va de 16 à 80 km en fonction des obstacles puisque le système fonctionne avec les ondes radio. Une sorte de talkie-walkie du futur ! Il est même possible de communiquer via SMS ou de vous géolocaliser par rapport à vos amis. Si vous partez faire de la randonnée, que vous aimez la voile ou que vous vous appelez Bear Grylls, la GoTenna est l'appareil qu'il vous faut d'autant qu'il ne s'agit pas d'un gadget de millionnaire. Les GoTenna sont vendues par deux et si vous en prenez 4 c'est encore moins cher. Attention le succès est tel qu'il faudra les commander à l'avance...



Prix : **120 € (les deux !)** Lien : www.gotenna.com

WiFi Stash,

UN LECTEUR DE CARTE SANS FILS

Ce petit gadget est un lecteur de carte multimédia (SD, TF/M2 et USB) qui fonctionne avec son propre réseau WiFi. Il permet, sans avoir accès à un réseau local, de partager des fichiers entre des appareils sous Android, iOS et PC sous Windows. Le WiFi Stash n'a même pas besoin d'être connecté au secteur (10 heures d'autonomie) pour fonctionner, mais qu'il le soit ou non, il fait aussi office de «powerbank». Vous pouvez donc recharger d'autres appareils en les connectant.

Prix : **25 €** Lien : www.chinavasion.com/gr88



THL 5000,

UNE BATTERIE DE COMPÉTITION

Le THL 5000 est un smartphone sous Android KitKat équipé d'une batterie d'une capacité exceptionnelle de 5000 mAh ! Alors que la concurrence ne propose généralement que des batteries aux alentours des 3000 mAh pour des appareils avec des écrans de 5 pouces, ce constructeur chinois frappe un grand coup. Cela permettrait au THL 5000 de tenir 1000 heures en veille, 47 heures en communication et 11 heures en mode «multimédia». Et n'allez pas croire que le reste des composants soit en retrait : processeur MediaTek MT6592 8 cœurs, 2 Go de mémoire vive et 16 Go de stockage interne extensibles via un port micro-SD. L'APN provient de chez Sony et l'écran, traité Gorilla Glass 3, propose une résolution de 1920x1080 pixels. Notons aussi que l'appareil peut recharger une autre machine depuis son port USB OTH et qu'il supporte le dual SIM.

Prix : **230 €** Lien : www.chinavasion.com/asnr



Call Recorder for mobile phone,

ENREGISTREZ VOS CONVERSATIONS MOBILES

Voici un appareil assez curieux permettant d'enregistrer des conversations téléphoniques que vous auriez sur votre téléphone portable. Une fois associé à votre appareil via Bluetooth, vous pourrez sauvegarder plusieurs heures de conversation sur les 8 Go de mémoire interne (extensible via carte Micro-SD). Attention, selon la loi française, votre interlocuteur doit être prévenu d'un éventuel enregistrement de sa voix.

Prix : **40 €**

Lien : www.chinavasion.com/dg4i

DANS CE MAGAZINE :

**[+ DE 80
TUTOS
& ASTUCES]**

EN - DE **5** MN
CHRONO !



POSOLOGIE :

- ☒ DE 1 À 5
ASTUCE(S) / JOUR
- ☒ PAS D'EFFET
SECONDAIRE
- ☒ EFFICACITÉ
GARANTIE
- ☒ NE CONTIENT QUE DES
INGRÉDIENTS GRATUITS



L 14376 - 4 - F: 3,50 € - RD



BEL/LUX : 4,60 € - DOM : 4,70 € - PORT. CONT. : 4,60 € -
CH : 6 FS - CAN : 6,99 \$ CAD - MAR : 43 MAD -
TUN : 6,4 TND - NCA/US : 620 CFP - POL/S : 660 CFP