100% PRATIQUE

[OVERCLOCK] Débrider son mobile

[TV & VIDÉOS] Passer à l'illimité

[C'EST POSSIBLE !] Ne plus payer ses applis

LES DOSSIERS DU

Pirate

3,50 € seulement

0% PUBLICITÉ

iPhone Android

HACKING ANONYMAT PROTECTION MULTIMÉDIA

80 HACKS POUR VOTRE SMARTPHONE

+ LE GUIDE DU ROOT SUR ANDROID & DU JAILBREAK iOS

SOMMAIRE

EN PARTENARIAT AVEC LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

DÉCRYPTAGE

HACKING

PROTECTION

ANONYMAT

CHIFFREMENT

MULTIMÉDIA

LES DOSSIERS DU **Pirate**

n°11 - Avril - Juin 2017

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

Directeur de la publication :
David Côme
Pinkman : Benoît BAILLEUL
Badger & Skinny Pete : Yann Peyrot & Thomas Povéda
Skyler & Gus : Stépanie Compain & Sergueï Afanasiuk
Correctrice : Marie-Line Bailleul

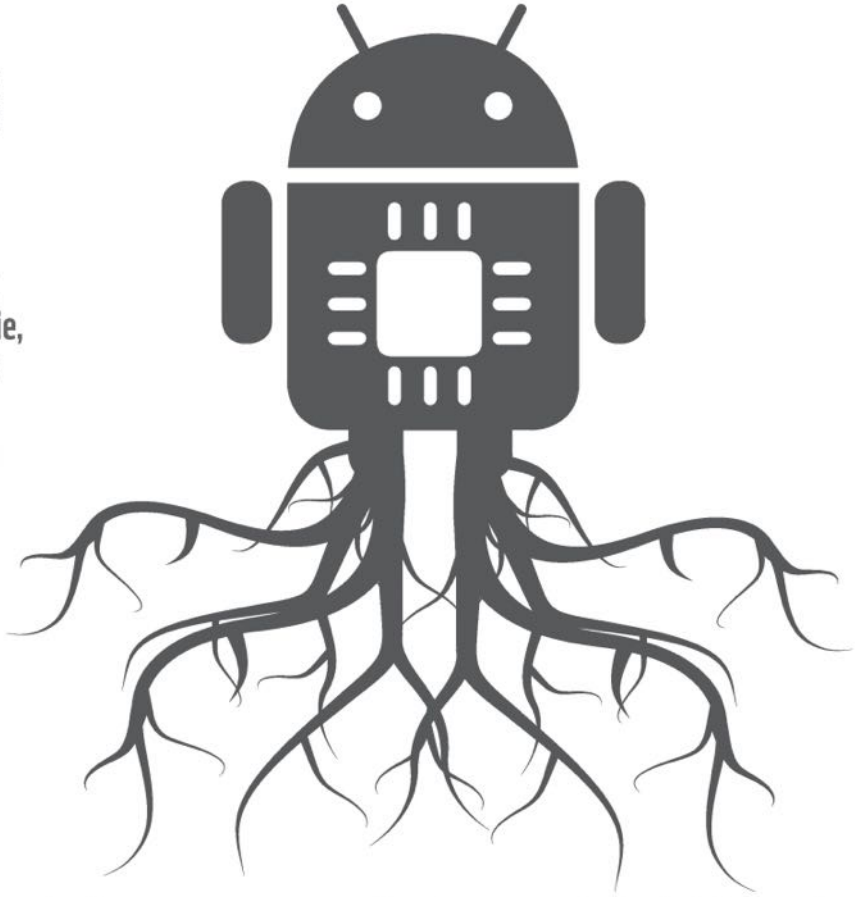
Imprimé en France par / Printed in France by :
Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 2267-6295

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

TOUT SAVOIR
SUR LE ROOT

Mais c'est quoi ce « root » dont tout le monde parle ? À quoi ça sert ? C'est risqué ? Ils disent que ça fait sauter ma garantie, c'est vrai ? Pas de panique, on vous dit tout, et même le reste !



Obtenir tous les droits sur son appareil Android. Voilà comment l'on peut définir le root. Par défaut, il n'est pas possible de modifier le système en profondeur, tout simplement pour éviter de l'endommager de manière irréversible. En rootant, vous faites sauter ces verrous. Dans la majorité des cas, le root passe par le déverrouillage du bootloader (programme qui permet de lancer un système d'exploitation, ici Android) de l'appareil, ce qui efface toutes les données de ce dernier. Notez qu'il n'existe pas de procédé universel. Si les méthodes présentées ici ne concernent pas votre appareil, une recherche de type « root [nom de l'appareil] » s'impose.

LE ROOT EST-IL LÉGAL ?

Oui. Rooter son appareil est tout à fait légal. Le code d'Android est en libre accès (« open source ») et l'opération

est d'ailleurs encouragée, du moment que vous n'utilisez pas vos nouveaux droits pour télécharger des applications illégales (une application payante devenue gratuite comme par magie, ou une qui permet de récupérer les données personnelles de quelqu'un à son insu). Le root seul n'est donc en aucun cas associé au piratage.

LE ROOT EST-IL RISQUÉ ?

Oui et non. Modifier un système d'exploitation en profondeur comporte toujours un risque, mais dans 99 % des cas, vous réussirez sans encombre... à condition de bien suivre les instructions. Ayez le réflexe de sauvegarder vos données (photos, musiques...) pour les retrouver en cas de problème. Et chargez bien votre appareil à fond avant de vous lancer. Dans le pire des cas, votre appareil sera « brické » : il ne fonctionnera plus du tout. Parfois, vous serez confronté à un « bootloop », un redémarrage en boucle du smartphone ou de la tablette. Les solutions à ce problème, dépendantes de l'outil utilisé, sont le plus souvent indiquées au sein des tutoriels.

FAUT-IL ROOTER POUR INSTALLER UNE ROM CUSTOM ?

Non. Si vous avez installé un mode Recovery alternatif (une interface de démarrage, comme ClockWorkMod ou TWRP), vous pouvez installer n'importe quelle ROM (un système d'exploitation alternatif) compatible avec votre appareil, sans root. 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 !

Un Moto X (2014) rooté sous Android 7.1.1, via la ROM CyanogenMod

LE ROOT DÉCUPLE LES CAPACITÉS DE VOTRE APPAREIL ANDROID !

LE ROOT FAIT-IL SAUTER LA GARANTIE ?

Non. La loi est claire à ce sujet. Si vous renvoyez votre appareil rooté encore sous garantie légale de conformité (2 ans après l'achat pour du neuf), c'est au vendeur de prouver que le root est à l'origine du problème. S'il ne le peut pas, il doit réparer/remplacer le smartphone ou la tablette sans frais.

ROOTER, POUR QUOI FAIRE ?

Si le root n'a plus de secret pour vous, encore faut-il savoir à quoi ça sert. Voici quelques exemples non exhaustifs pour vous convaincre de l'utilité de l'opération.

« J'en ai marre de ces pubs plein écran dans les applis ! » « T'as qu'à rooter ton smartphone ! » « Ah parce que ça sert à ça ? » Oui, et pas que ! Le root, c'est la porte d'entrée dans un monde de possibilités. La plus flagrante est l'accès aux nombreuses applications du Google Play Store estampillées « root only ». Plus concrètement, vous pouvez aussi :

> Supprimer les applications préinstallées

Un appareil Android est toujours vendu avec des applications impossibles à désinstaller (les applis Google, Facebook, les applis Samsung, HTC ou autre...). Avec un appareil rooté, désinstallez-les comme n'importe quelle autre ! Utilisez **Ccleaner** sur Android par exemple.

> Supprimer la publicité

Peut-être la fonction la plus recherchée. La pub sert à rémunérer les développeurs qui proposent une application gratuite, sauf que certains abusent clairement (popup en plein écran ou bannière gênante). **Adaway** bloque les publicités sur le Web et dans les applis... si vous êtes rooté.

>Augmenter l'autonomie ou les performances

Le root permet un contrôle total sur le système, et donc sur les composants de l'appareil.
Des applications peuvent gérer finement les ressources allouées au processeur suivant les cas, pour économiser la batterie. De la même manière, il est possible d'overclocker le processeur.

> Récupérer des photos supprimées par erreur

Même si l'opération est possible sans root via certaines applications comme **Dumpster** (à condition de l'avoir installée AVANT de perdre vos photos), être rooté facilite grandement la tâche, puisque l'appli va pouvoir «fouiller» dans plus de fichiers, et donc augmenter les chances de récupération.

> Mettre à jour son appareil

Chaque nouvelle version d'Android laisse sur le carreau certains appareils, jugés trop «vieux» pour recevoir la mise à jour. Grâce aux ROM Custom, même un Moto X (2014), normalement bloqué à Android 6.0 Marshmallow, peut profiter d'Android 7.0 Nougat !

> Installer des ROM Custom

Un changement radical ! vous remplacez le système d'exploitation par un autre, souvent garni de fonctionnalités supplémentaires et d'amélioration des performances.
Nous l'avons dit : il n'est pas obligatoire d'être rooté pour changer de ROM, mais pour utiliser la plupart de leurs fonctions, oui.

> Sauvegarder tout son appareil

Il est possible de sauvegarder l'ensemble de votre appareil (médias, SMS, journal d'appels, données d'applications, préférences...) sans root, mais il faut multiplier les applications.
Une fois rooté, **Titanium Backup** (par exemple) se charge de tout en quelques clics.

INFOS [**ODIN**] Où le trouver ? [**http://odindownload.com**]
[**CF-AUTO-ROOT**] Où le trouver ? [**https://autoroot.chainfire.eu**]
Difficulté : ☠☠☠

ROOTER UN APPAREIL SAMSUNG, NEXUS OU AUTRE

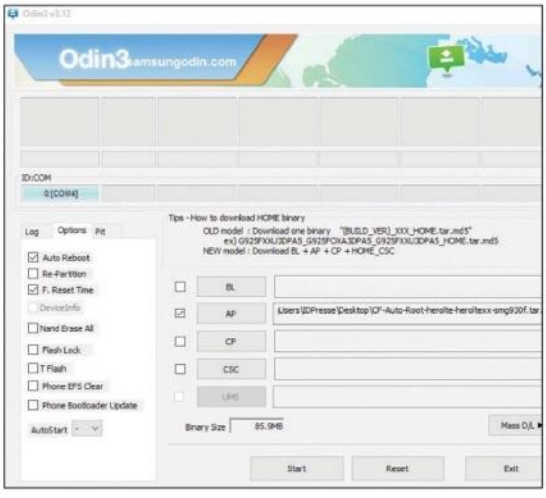
PRATIQUE

01 › TÉLÉCHARGER LES OUTILS

Sur votre PC, téléchargez la dernière version d'**Odin** et l'archive **CF-Auto-Root** correspondante à votre modèle (ne vous trompez pas). Nous avons pris l'exemple du Galaxy S7. Décompressez le dossier CF-Auto-Root pour récupérer un fichier terminant par **.tar.md5** (les autres fichiers ne seront pas utilisés).

02 › PRÉPARER L'APPAREIL MOBILE

Dans les **Options développeurs (Paramètres > À propos du téléphone/de la tablette >** appuyez 7 fois sur **Numéro de build** et revenez en arrière), activez le **Déverrouillage OEM** et le **Débogage USB**. Sauvegardez tous les fichiers importants (le mobile sera effacé pendant la procédure). Assurez-vous que l'appareil est chargé à 100% et redémarrez-le en mode **Download** (restez appuyé sur les boutons **Home**, **Power** et **Volume bas** en même temps).



03 › ROOTER L'APPAREIL

Ouvrez **Odin** et connectez l'appareil mobile au PC avec un câble USB. La case sous **ID:COM** devient bleue. Cliquez sur **AP** et sélectionnez le fichier terminant par **.tar.md5**. Dans l'onglet **Options**, cochez les cases **Auto Reboot** et **F. Reset Time**, puis décochez **Re-Partition**. Lancez le root avec **Start**. Patientez jusqu'au redémarrage de l'appareil, désormais rooté.

ATTENTION À KINGO ROOT !

Le célèbre outil de «root en un clic» **Kingo Root** marche bien et couvre pas mal d'appareils, mais des utilisateurs font état de processus étranges sur leur smartphone et d'envois de données vers la Chine... Nous vous conseillons plutôt, en plus d'Odin, **Windows Universal Android Toolkit**. Un tuto vidéo est disponible ici : **https://goo.gl/hBcR9P**.

NUMÉRO EXCEPTIONNEL

LE GUIDE 100% TABLETTES

3,90 € seulement

+ DE 80 TUTOS POUR VOTRE TABLETTE ANDROID

CHEZ VOTRE MARCHAND DE JOURNAUX

JAILBREAK D'IOS : POURQUOI ET COMMENT ?

Sujet à la mode il y a quelques années pour les détenteurs d'iPhone, le jailbreak n'est plus aussi en vogue qu'à l'époque. Il reste pourtant utile pour qui veut libérer son appareil Apple.

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 donne une vraie bouffée d'air frais aux « Apple addicts ».

JAIL QUOI ?

Le jailbreaking consiste 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. Par exemple

: personnaliser l'interface, installer des applications que ne viennent pas forcément de l'AppStore, émuler des consoles de jeux...

LE JAILBREAK VAUT-IL ENCORE LE COUP ?

Très prisé à l'époque, le jailbreak n'a plus le vent en poupe. D'abord parce qu'Apple a, au fil des mises à jour de son OS, intégré de plus en plus de fonctions auparavant réservées aux appareils jailbreakés (mode « nuit », commandes vocales personnalisées...). Ensuite parce que la firme est de plus en plus réactive pour combler les failles de sécurité permettant l'opération. Les développeurs de jailbreak se découragent et des équipes célèbres comme Pangu n'ont rien proposé depuis iOS 9.3.3. Pourtant, le jailbreak permet encore plein de petits « tweaks » (modifications) absents d'iOS : explorateur de fichiers complet, possibilité de se passer de l'appli Messages, configuration fine du son, nettoyeur à la CCleaner...

LA MÉTHODE

Au moment de rédiger cet article, Apple venait de diffuser la version 10.2.1 de son OS, empêchant le jailbreak mis au point par le développeur Yalu pour 10.2. Nous nous sommes donc procuré un iPhone sous 10.2 pour le tutoriel de la page suivante. Si Yalu propose un jour un jailbreak pour 10.2.1 (ou plus), la manipulation sera exactement la même. Il faudra juste télécharger le bon fichier sur son site (cf. étape 1). Avant de commencer, assurez-vous d'avoir la dernière version d'iTunes sur votre PC et d'avoir branché au moins une fois l'iPhone à ce dernier pour **Se fier** à l'ordinateur (touchez cette option sur l'iPhone). Profitez-en pour faire une sauvegarde de l'appareil, au cas où vous devriez revenir en arrière. Enfin, notez que le jailbreak présenté ici est un « semi-untethered ». Comprenez qu'il faudra effectuer la dernière étape du tutoriel chaque fois que vous éteignez et rallumez l'iPhone. Il s'agit juste de lancer une application, rien de très contraignant.

LE JAILBREAK PERMET AUX UTILISATEURS D'IPHONE D'OUTREPASSER LES LIMITES IMPOSÉES PAR APPLE...

LÉGAL OU PAS ?

Le jailbreak n'est pas interdit, mais utiliser cette manipulation pour télécharger des applications payantes gratuitement reste illégal, puisque cela s'apparente à du piratage. Apple est encore plus strict : *« 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 »*. Les logiciels de jailbreak contiennent en effet des pans de code qui appartiennent à la société. Apple a donc décrété que l'opération ferait automatiquement sauter la garantie.

INFOS [YALU102]

Où le trouver ? [**https://yalu.qwertyoruiop.com**]

Difficulté :

LE JAILBREAK AVEC YALU102

PRATIQUE

01 › RÉCUPÉRER LES OUTILS NÉCESSAIRES

Le jailbreak présenté ici est encore en bêta. Il fonctionne uniquement à partir de l'iPhone 5S et au-delà, mais pas pour les iPhones 7 et 7 Plus. Sur

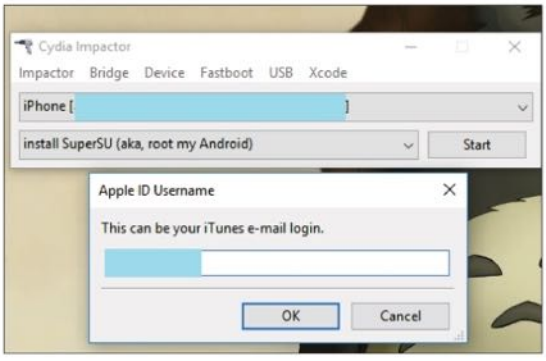
votre PC ou Mac, téléchargez la dernière version du fichier **.ipa** sur le site suivant : **https://yalu.qwertyoruiop.com,** puis la dernière version de **Cydia Impactor**, en fonction de l'OS de l'ordinateur, depuis ce site : **www.cydiaimpactor.com**.

02 › PRÉPARER L'IPHONE

Allez dans **Réglages > Touch ID et code** puis désactivez **Déverrouiller l'iPhone** et **iTunes Store et App Store**. Toujours dans les **Réglages**, allez dans **iCloud > Localiser mon iPhone** et désactivez cette option (il faudra entrer votre mot de passe Apple pour valider). Par sécurité, branchez l'iPhone à l'ordinateur et utilisez **iTunes** pour faire une sauvegarde de l'appareil (**Sauvegarder maintenant**).

03 › INSTALLER YALU102

Si ce n'est pas déjà fait, branchez l'iPhone à l'ordinateur. Ouvrez **Cydia Impactor** et faites



glisser le fichier **.ipa** dans la case du haut. Entrez votre identifiant Apple, cliquez sur **OK**, puis faites de même avec votre mot de passe. L'opération démarre automatiquement. Attendez que la fenêtre de **Cydia Impactor** affiche **Complet** et débranchez l'iPhone du PC. L'appli yalu102 est installée.

04 › JAILBREAKER L'IPHONE

Allez dans **Réglages > Général > Gestion des appareils**. Touchez la ligne sous **App de développeur**. Elle porte généralement le nom de votre compte Apple. Touchez f**aire confiance à...** et **Se fier**, puis revenez sur le bureau. Ouvrez l'application **yalu102** et appuyez sur **go** pour lancer le jailbreak. Attendez que l'iPhone redémarre. Cydia est désormais installé, et vous êtes jailbreaké !

CYDIA : VOTRE NOUVEL APP STORE

L'installation de Cydia est la preuve que la tentative de jailbreak a bien fonctionné. Il est temps de plonger dans ce monde de nouvelles possibilités.

Vous avez suivi le tutoriel de la page précédente et votre iPhone est enfin libéré de ses chaînes, félicitations ! Mais on fait quoi maintenant ? On ouvre Cydia et on profite de toutes ces applications et fonctionnalités utiles qui font défaut à iOS. L'avantage de Cydia, c'est la possibilité d'ajouter ses propres sources. Comprenez que ce magasin est un répertoire ouvert, et que chacun peut compiler et proposer ses applis, sous forme de « repos ». Il faudra ajouter ces « repos » à Cydia par une manipulation très simple détaillée page suivante.

DU BON, DU BRUT ET DU TRUAND

De base, Cydia est fourni avec plusieurs sources connues et approuvées. Vous avez donc largement de quoi faire. Si l'envie vous prend d'ajouter un nouveau « repos », faites attention à sa provenance (rendez-vous page 27 pour une sélection de sources). D'une manière générale, les applis proposées sont abouties et stables, mais on trouve aussi des projets en cours de développement, instables, et des applis payantes devenues gratuites (piratées donc, pour ceux qui ne suivent pas au fond). Cydia affiche d'ailleurs un avertissement quand vous tentez d'installer une source connue pour cela. Dans tous les cas, sachez que les sources doivent être mises à jour comme n'importe quelle application. Voyons cela ensemble.

INFOS [CYDIA IMPACTOR]

Où le trouver ? [**www.cydiaimpactor.com**]

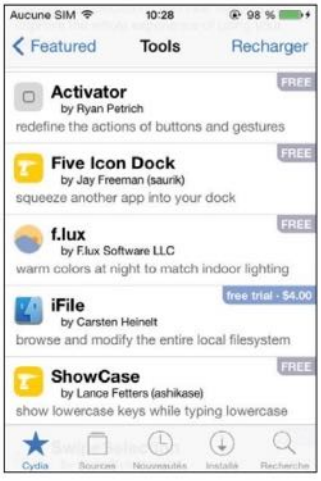
Difficulté :

EXPLOITER CYDIA

PRATIQUE

01 › FAIRE LE TRI

Cydia n'est pas le magasin d'applications le plus ergonomique du monde. Commencez par toucher **Sélection** pour obtenir des catégories. **Outils pour débuter**, **Personnalisation de l'interface**, **Solutions anti-tracas**... Si vous ne cherchez rien de particulier, c'est par là qu'il faut passer. Il n'y aura pas beaucoup de choix, mais vous n'aurez que le meilleur.



02 › INSTALLER UNE APPLICATION

Rien de bien sorcier ici. Touchez l'appli qui vous intéresse puis **Installer** et **Confirmer**. Attendez que l'opération se termine et finissez avec **Relancer le SpringBoard**. Suivant les cas, il faudra appuyer sur **Modifier** puis **Installer**. Pour désinstaller l'appli, l'opération est la même, mais il faudra choisir **Supprimer** avant de **Confirmer**.

03 › AJOUTER UNE SOURCE

Vous avez trouvé une source de confiance pour ajouter des applications à Cydia ? Allez dans

Sources > Modifier > Ajouter (en haut à gauche) et entrez l'adresse du « repos ». Validez avec **Ajouter la source**. Si un avertissement apparaît, touchez **Ajouter quand même**. Terminez par un **Retour vers Cydia**.

04 › METTRE À JOUR LES SOURCES

Cydia vous avertit de lui-même quand des sources ont besoin d'être mises à jour. Sur le popup, touchez **Mise à niveau OK**. Il est conseillé de le faire dès que vous en avez l'occasion pour éviter tout dysfonctionnement.

LE FORUM

DE LA COMMUNAUTÉ

Android MT

forum.android-mt.com

Tutoriels · Conseils & astuces · Tests · Avis ·
Dépannage · Hacking · Découverte d'applications...

HACKING

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 Linux puisqu'avec un mobile sous Android et cSploit, vous pourrez lancer toute une batterie de tests : sniffing, sidejacking, crack de mot de passe, etc.

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. cSploit est une application fonctionnant avec n'importe quel appareil rooté (voir page 4).

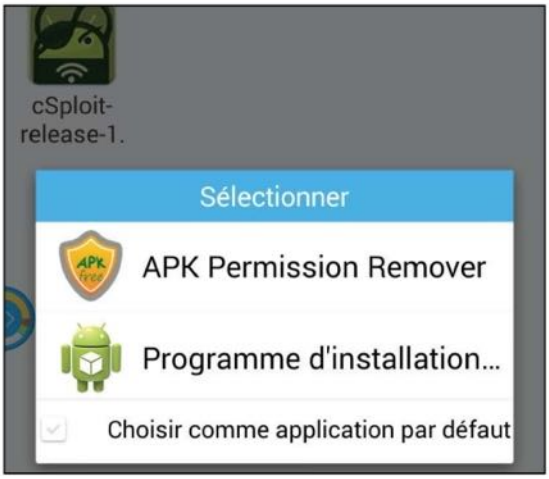
TOUTE UNE SUITE DE LOGICIELS POUR TESTER ET SÉCURISER UN RÉSEAU !

DES VULNÉRABILITÉS CONNUES, MAIS PAS FORCEMENT COLMATÉES

Vous pourrez alors rechercher dans votre réseau les vulnérabilités matérielles et logicielles connues, scanner les ports, sniffer des mots de passe, manipuler le trafic et 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...

INFOS [CSPLOIT]
Où le trouver ? [**http://www.csploit.org**]
Difficulté : ☠☠☠

LES FONCTIONNALITÉS DE CSPLOIT



01› INSTALLATION

cSploit n'est pas disponible sur le Google Play Store, il faudra télécharger le fichier APK depuis cette adresse(**http://www.csploit.org**) puis le transférer via le câble USB, le Bluetooth ou vous l'envoyer par mail. Pour pouvoir l'installer, il faudra autoriser les sources inconnues. Allez dans **Paramètres>Sécurité** et cochez **Sources inconnues**. Si vous n'avez pas l'outil BusyBox, l'appli vous la demandera peut-être en fonction de votre version d'Android.

02› MAPPAGE DU RÉSEAU

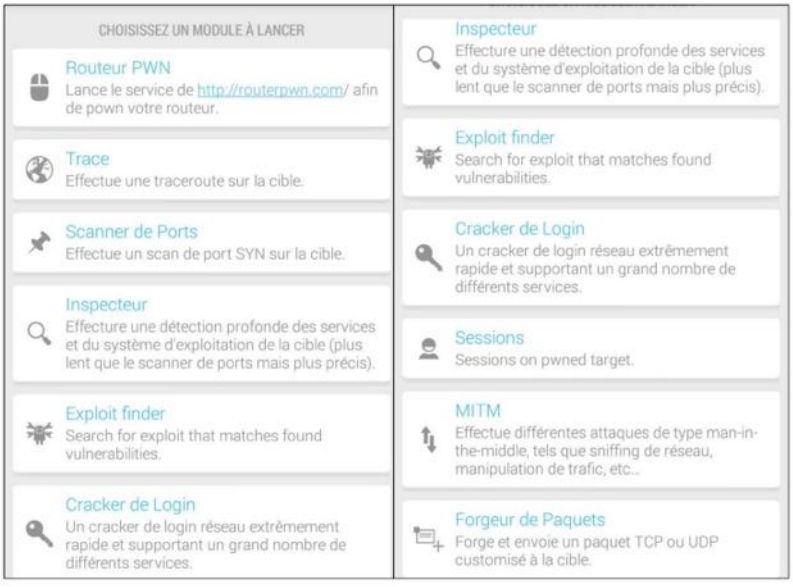
Accordez les droits root **Super User** et mettez à jour le Core si on vous le demande. Dès le lancement, vous verrez tous les périphériques qui sont connectés à votre réseau local, y compris votre smartphone et votre box/routeur avec leur IP, adresse Mac, un descriptif et les ports utilisés. Choisissez-en un pour voir les options qui correspondent.

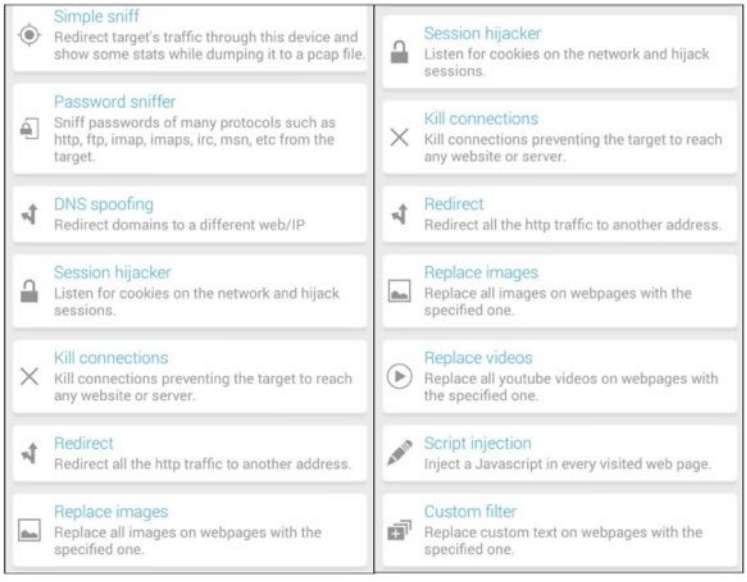
ET DU CÔTÉ DE LA POMME ?

Vous devez vous en douter, mais vous ne trouverez pas d'application de ce type sur l'App Store. Cependant, vous pouvez trouver énormément de sources sur Cydia si vous avez eu la bonne idée de jailbreaker votre appareil (voir page 10). Citons **Tcpdump** pour capturer le trafic (comme Wireshark sur PC), **GNU Debugger** pour le reverse engineering ou des outils connus comme **Metasploit**. Pour accéder à ces applications, il faudra ajouter le dépôt iNinja avec Cydia. Si vous êtes perdu, voici un tuto pour vous y retrouver : **https://goo.gl/0Jxc0P**.

03 › LES FONCTIONNALITÉS

Les fonctionnalités sont assez riches et dépendent du périphérique sélectionné. Avec notre routeur par exemple, le premier choix vous permet de donner accès au site **Routerpwn.com** qui liste les vulnérabilités liées aux routeurs du marché puis **Traceroute** qui permet de suivre les paquets d'informations sur le réseau puis un **Scan de ports standard** et poussé (**Inspecteur**). Viennent ensuite les recherches de vulnérabilités connues (pratique pour un PC sous Windows) et un module de cracking.





04 › ENCORE PLUS DE TESTS...

En bas de ce menu, vous trouverez aussi l'option MITM (Man-in-the-Middle) qui offre encore plus de tests: sniff de mots de passe (récupération à la volée), redirection de DNS et le **Session hikacking** qui permet de voler l'accès à un site protégé par mot de passe. Vous pouvez aussi utiliser l'ARP poisoning pour interdire la connexion à un périphérique ou troller un ami en changeant toutes les images des sites consultés par des photos de François Hollande...

INFOS [Lucky Patcher]
Où le trouver ? [**www.luckypatchers.com/download**]
Difficulté : ☠☠☠

LUCKY PATCHER : NE (RE)PAYEZ PLUS VOS APPLIS !

Soyons clairs, Lucky Patcher est une application qui ouvre la voie au piratage. Il s'agit en fait de contourner la vérification de la licence d'une appli ou d'un jeu. Nous préférons voir cette méthode comme un moyen de récupérer des droits sur une application que vous auriez déjà payée par exemple ou de permettre de tester plus sérieusement une appli très chère...

Les systèmes Android et iOS fonctionnent avec des fichiers qui viennent s'installer sur votre smartphone ou tablette un peu comme un EXE vient s'installer sur Windows. Mais là où on vous demandera une clé de licence sur PC, Google enregistre votre achat et vous transfère une licence numériquement signée que vous seul pouvez utiliser sur votre machine. Lorsque vous perdez votre téléphone par exemple, Google ou Apple vous donne l'occasion de télécharger une nouvelle fois vos applis avec les licences, mais imaginez que vous perdiez aussi vos identifiants... Dans ce cas vous perdez votre compte et vos précieux achats.

CONTOURNER LES VÉRIFICATIONS DE LICENCE

Si votre appareil est rooté (voir page 4) ou jailbreaké (voir page 10), Lucky Patcher va simplement contourner la vérification des licences sur votre machine pour lancer les applis que vous avez déjà achetées. Bien sûr cette méthode permet aussi à des petits malins de lancer des applications qu'ils n'ont jamais payées. Mais après tout, pourquoi ne pas utiliser Lucky Patcher pour tester la version complète d'une appli avant de dépenser son argent ? Les versions démos sont souvent bridées et il est parfois difficile de se faire un avis définitif avec une version limitée... Notons aussi que Lucky Patcher peut aussi supprimer les publicités des applications gratuites, outrepasser les périodes d'essai, changer les permissions et sauvegarder les applis modifiées.

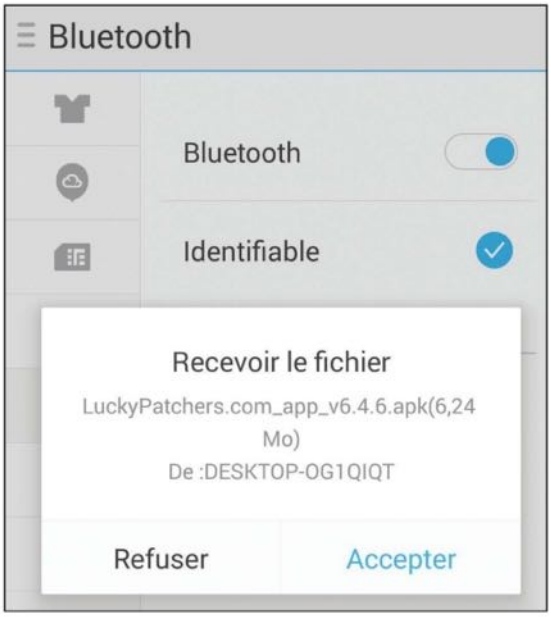
UN CONTRÔLE TOTAL SUR TOUTES VOS APPLIS !

INFOS [Lucky Patcher]
Où le trouver ? [**www.luckypatchers.com/download**]
Difficulté : ☠☠☠

CONTOURNEMENT DE LICENCE AVEC LUCKY PATCHER

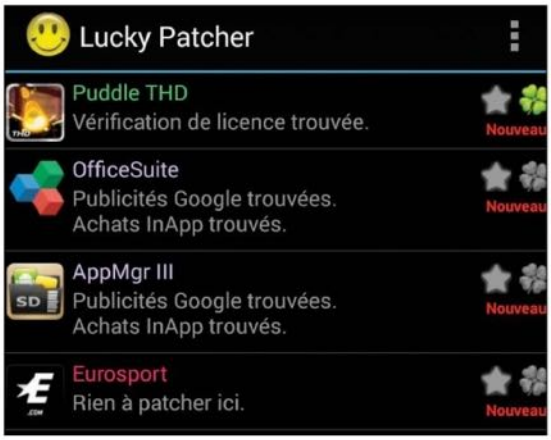
01 › PRÉ-REQUIS

Téléchargez et installez Lucky Patcher sur votre appareil rooté (on vous demandera aussi sans doute d'installer la Busy Box). Sur le Net vous trouverez des applications aux formats APK avec des dossiers de licence qui commencent par **com**. Il faudra suivre les instructions contenues dans le fichier texte, mais la plupart du temps le procédé sera le même.



02 › LES OPTIONS

Installez l'APK de l'application que vous convoitez, mais surtout ne la démarrez pas (vous pouvez aussi utiliser ce service pour récupérer l'APK depuis un PC: https://apps.evozi.com/apk-downloader). Dans notre cas nous essaierons d'installer le jeu Puddle. Sans Lucky Patcher, le jeu refusera de démarrer, car la licence n'est pas valide. Lancez Lucky Patcher et faites un appui long sur Puddle. Dans la liste des actions, vous pourrez notamment **Supprimer les publicités**, **Créer un .apk modifié** (pour intégrer un patch directement à l'APK) ou geler une application qui pomperait trop de ressource.

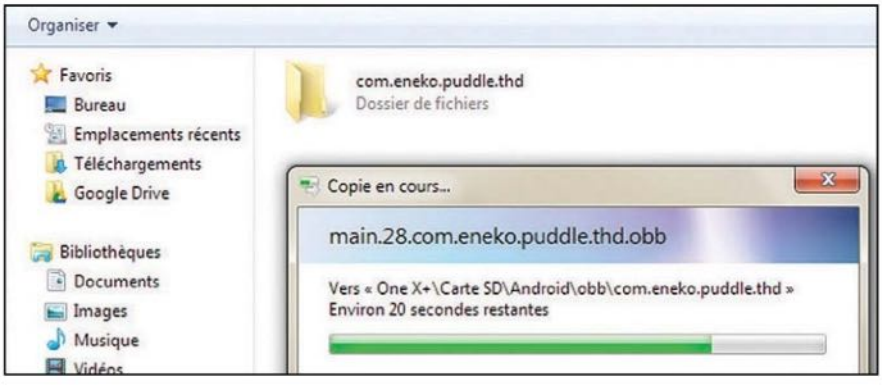


03 › SUPPRESSION DE LA VÉRIFICATION

Mais ce qui nous intéresse ici c'est **Supprimer la vérification de licence**. Utilisez le mode **Auto** et attendez que Lucky Patcher aille chercher le patch adéquat (il vous faudra une connexion à Internet durant cette étape). A la fin, l'appli vous donnera une approximation de la réussite de la manipulation. Dans notre cas, Puddle avait 42% de chance de se lancer.

04 › LANCER VOTRE APPLI

Selon l'appli que vous voulez faire fonctionner, il vous sera aussi demandé de copier à la main les dossiers d'une licence (qui fera office de «carte blanche»). Copiez le dossier dans **/sdcard/Android/Obb** et lancez enfin votre application. Dans notre cas, et même avec seulement 42% de chance, le jeu se lance. Notez qu'il s'agit de la version complète ! Lucky Patcher ne fonctionne pas avec votre fichier APK ? Pas de panique, les développeurs ajoutent des patchs tous les jours !



INFOS [NO-FRILLS CPU CONTROL]

Où le trouver ? [**https://goo.gl/79MJOT**]

Difficulté :

UN PORTABLE À PLEINE PUISSANCE !

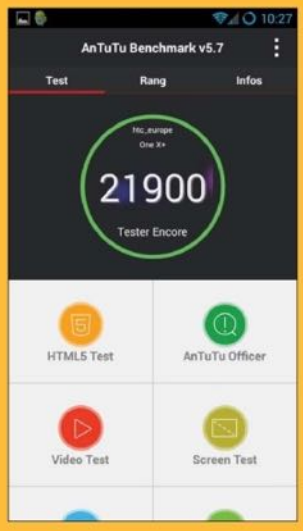
Nos chers smartphones et tablettes sont de plus en plus puissants et embarquent toujours plus d'électronique très avancée. Sur des appareils rootés il est possible d'overclocker le processeur pour améliorer les performances, mais aussi de faire l'inverse pour économiser de la batterie...

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 criera famine...

PLUS QU'UN OVERCLOCK, NO-FRILLS PERMET DE PARAMÉTRER VOTRE CPU EN FONCTION DE VOTRE UTILISATION

ANTUTU CPU MASTER, LE CONCURRENT



Si No-Frills ne vous a pas convaincu, pourquoi ne pas essayer son concurrent ? Comme son alter-ego, ce dernier n'autorisera pas la mise en danger de votre appareil (un overclock trop élevé peut faire chauffer la machine et la détériorer). Vous ne pourrez qu'augmenter la valeur minimale (**Min**). Appuyez ensuite sur **Apply**. Les tâches courantes seront donc expédiées plus rapidement, mais vous pourrez aussi baisser la cadence pour économiser de la batterie. Pour comparer les résulats entre vos réglages ou entre vos appareils, AnTuTu propose aussi une appli de banc d'eesai : AnTuTu Benchmark. Bien sûr, c'est gratuit !

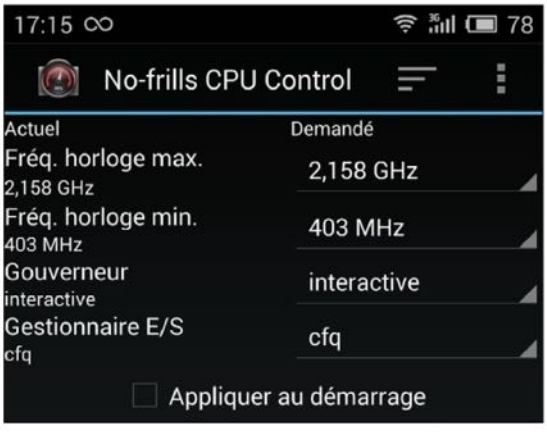
Lien : https://goo.gl/u8wTSO

LE CHOIX DE LA PUISSANCE AVEC NO-FRILLS CPU CONTROL

PRATIQUE

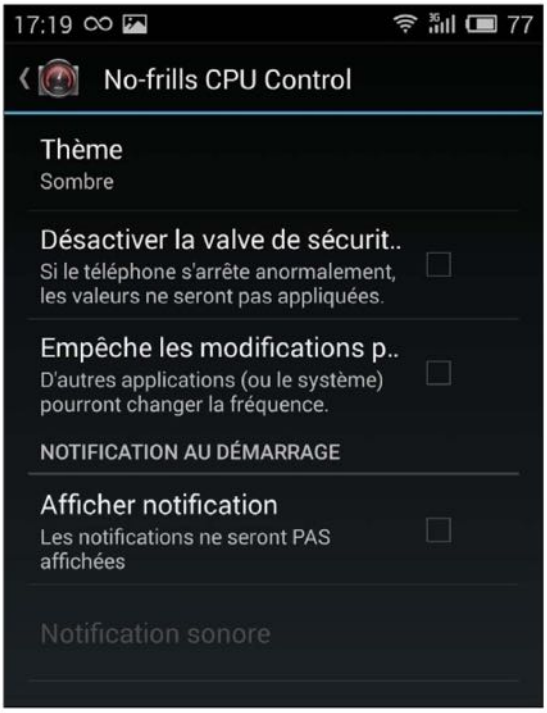
01 › L'INTERFACE

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.



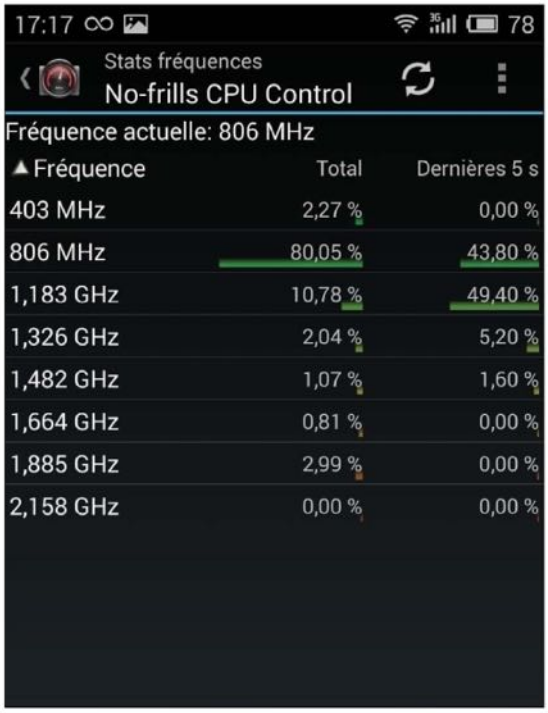
02› LES STATISTIQUES

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.



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 DU CÔTÉ DE LA POMME ?

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). Pour les petits bidouilleurs, vous pouvez toujours tenter iOverclock que vous trouverez sur le marché alternatif Cydia.

LES MEILLEURES ALTERNATIVES AUX APP STORE OFFICIELS

Android a son Google Play Store et iOS a son App Store. Mais que les amateurs de changements se rassurent : les marchés d'applications alternatifs sont nombreux ! Voici les meilleurs du genre.

On a beau dire qu'Android est plus ouvert qu'iOS, il y a un point sur lequel l'OS au robot vert rejoint son concurrent dans l'exclusivité : le magasin d'applications. Avec les centaines de millions d'applis disponibles, on a vite fait d'oublier que les alternatives existent, et qu'elles sont très intéressantes ! Applications open source, introuvables ailleurs, réductions sur le payant... Sur Android, le changement vaut le coup. Sur iOS, c'est plus compliqué.

LE CAS CYDIA

Pour sortir de l'App Store, les amateurs de la pomme n'ont pas vraiment le choix : jailbreak et installation de Cydia sont des étapes obligatoires. Cydia agissant comme un catalogue (avec du gratuit et du payant) auquel vous pouvez ajouter des « repos » (un répertoire contenant de nouvelles applis), il est virtuellement infini, ce qui explique le manque d'alternatives crédibles. Dans tous les cas, la prudence est de mise. Les applis n'étant pas vérifiées par Google ou Apple, c'est la porte ouverte aux hackers qui en veulent à votre appareil. Rappelez-vous enfin qu'utiliser ces magasins alternatifs pour télécharger une application payante devenue gratuite par l'opération de Saint Cook et Saint Pichai est illégal.

3 ALTERNATIVES SÉRIEUSES AU GOOGLE PLAY STORE

APTOIDE

La référence. Sur Aptoide, on trouve les applications du Google Play Store, mais aussi celles qui n'y figurent pas. Ce sont les utilisateurs qui proposent les applis. Chacun peut les tester et les noter pour signaler d'éventuels bugs, voire des applis vérolées. Vous pouvez « suivre » une personne pour être tenu au courant de ces derniers uploads. Aptoide est rempli d'applications payantes devenues gratuites. Soyez vigilant.

F-DROID

F-Droid, c'est un peu le Framasoft d'Android. Plus précisément, son catalogue n'est composé que de FOSS (Free and Open Source Software). Il est donc moins étoffé que les autres, mais vous avez tout le loisir d'examiner le code de chaque application postée. Utiliser F-Droid permet surtout de profiter des mises à jour automatiques des applications. Si vous les téléchargez sans passer par F-Droid, il faudra à chaque MàJ récupérer la nouvelle APK, ce qui peut vite devenir fastidieux.

AMAZON UNDERGROUND

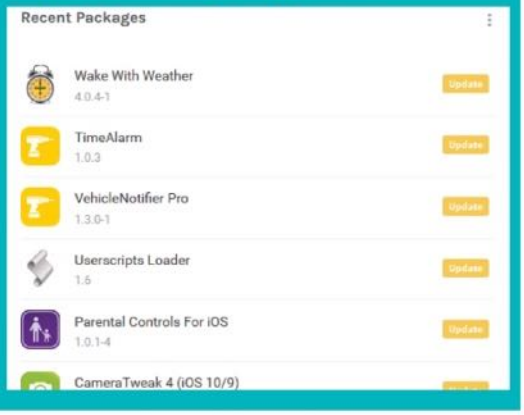
Le géant du commerce en ligne possède son propre magasin d'applications Android. Couplé à la possibilité de faire son shopping, il intègre les mêmes applis que sur le Google Play Store. En revanche, vous avez droit à une ou plusieurs applications(s) offerte(s) par jour, ce qui devient vite intéressant quand il s'agit d'un jeu normalement vendu 5 €. Notez qu'il faut se connecter à son compte Amazon pour télécharger les applications.

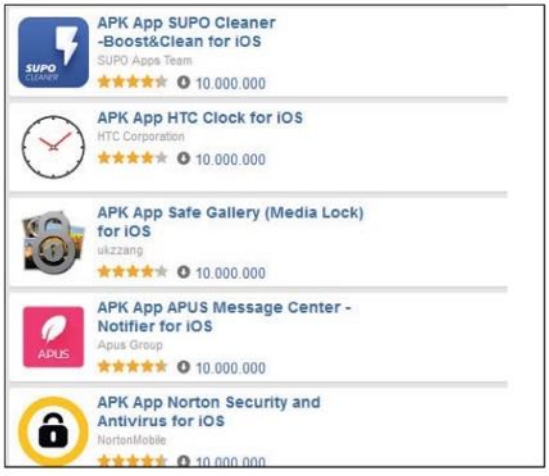
3 SOURCES INCONTOURNABLES POUR CYDIA

BITEYOURAPPLE

L'un des premiers « repos » que les utilisateurs de Cydia rajoutent au catalogue. BiteYourApple possède près de 8000 « packages » (applications) à lui seul. Si vous hésitez, le site Web classe le tout par catégorie, pour repérer rapidement ce qui vous intéresse. Comme sur un vrai magasin d'applications, chacune peut être notée et commentée.

http://repo.biteyourapple.net





APPCAKE

Si l'on vous parle d'AppCake, c'est bien sûr pour vous mettre en garde : ce répertoire Cydia est célèbre pour contenir uniquement des applications crackées. En plus de faire la part belle au payant devenu gratuit, AppCake permet de télécharger les applis volumineuses via torrent. Vous êtes désormais prévenus...

http://cydia.iphonecake.com

XSELLIZE REPO

Amateurs de jeux mobiles, ce « repos » est fait pour vous ! C'est en effet pour ce genre d'applications qu'xSellize est surtout connu. Ce qui ne l'empêche pas de proposer également des outils intéressants comme des bloqueurs de publicités ou des activateurs de fonctionnalités intégrés à l'iPhone mais inaccessibles par défaut, etc.

http://cydia.xsellize.com

INFOS [WIBR+]

Où le trouver ? [**http://auradesign.cz/android/wibrplus.apk**]

Difficulté : ☠☠☠

CRACK DE VOTRE RÉSEAU WIFI !

Le crack de mots de passe est un sujet tabou dans la presse informatique. En effet, cette technique est souvent associée aux pirates alors qu'il s'agit aussi d'un moyen de vérifier la sécurité de ses sésames. À la rédaction, nous avons donc décidé de vous montrer comment utiliser Wibr+, une appli spécialisée dans le crack de mots de passe WiFi.

UN SÉSAME BLINDÉ !

Comment savoir si vos mots de passe sont sûrs ? Nous avons déjà abordé le sujet par le passé en expliquant qu'un sésame doit être à la fois long, ne rien vouloir dire (pas un mot pouvant se trouver dans un fichier dictionnaire donc) et alterner les lettres majuscules, minuscules, chiffres et autres caractères spéciaux ($, ^, µ, &, etc.). Ces précautions sont primordiales pour qu'une personne ne devine pas votre mot de passe trop facilement, mais aussi pour contrer les applis comme Wibr+. Pour savoir si votre mot de passe est solide, une seule adresse : **https://howsecureismypassword.net**

Cracker un mot de passe consiste à le deviner en utilisant des outils informatiques et son cerveau (eh oui, il faut les deux). Il existe de nombreux outils sur PC (Windows et Linux) que nous vous présentons parfois dans *Pirate Informatique* et les *Dossiers du Pirate,* mais pour ce «spécial smartphone», nous avons jeté notre dévolu sur Wibr+, une appli bannie du Google Play Store. Cette dernière propose de casser le mot de passe d'un réseau WiFi pour y pénétrer. Bien sûr nous présentons cette appli pour tester votre propre réseau et aussi pour vous montrer comment s'y prennent les pirates pour accéder à votre réseau et l'utiliser pour réaliser tout un tas de méfaits (téléchargement illégal, attaque DDoS, etc.)

DEUX TYPES D'ATTAQUES

Wibr+ propose 2 types d'attaques. La première, dite par «dictionnaire», va essayer tout un tas de mots de passe puisés dans un fichier texte (voir notre encadré) en espérant y trouver le bon. Il faut savoir que de nombreuses personnes

changent le mot de passe par défaut de leur box/routeur (c'est une bonne idée) pour en choisir un plus simple et facile à retenir (c'est une très mauvaise idée). Les dictionnaires que l'on trouve sur Internet vont se concentrer sur ces mots de passe «passoires»: **azerty**, **jésus**, **123456**, **secret**, **bonjour**, **PSG**, etc. Attention, car ces mots seront différents dans certains autres pays. Pas sûr que **jésus** ait la côte en Israël ! De même les Anglo-saxons iront taper **qwerty** au lieu d'**azerty**. D'où l'importance de bien choisir son dico... La bonne chose avec cette méthode, c'est que lorsque le logiciel a épuisé le dictionnaire, vous êtes sûr que le mot de passe ne se trouve pas dedans. Il faudra alors changer de fichier ou passer à la méthode brute force...

LA MÉTHODE «BRUTE FORCE»

Avec cette technique, le logiciel va essayer tous les mots de passe possibles en commençant par exemple par **aaaaaa** puis **aaaaab**, **aaaaac**, etc. Plus le mot de passe est long et plus il comporte de types de caractères différents et plus il sera difficile de le découvrir. C'est d'autant plus vrai avec cette version Android puisque l'appli va tenter d'envoyer des mots de passe à un rythme très lent. En effet sur PC, on doit capturer un «handshake» et l'analyser pour en extraire le mot de passe. Cela permet de tester des milliers de mots de passe en quelques secondes. Ici, il faudra se contenter d'une quinzaine de clés par minute. Si le mot de passe à deviner est **Fg7^mP586/*P)ç-Hjj**, ce sera bien difficile, mais si c'est **toto75**, le crack sera vite expédié. Attention, l'appli occupe un maximum de ressource et votre batterie va se décharger à vue d'oeil ! Dans notre prise en main, nous allons voir comment utiliser et optimiser Wibr+...

TROUVER DES DICTIONNAIRES

Il n'est pas très difficile de trouver des dictionnaires sur Internet, mais encore faut-il utiliser le bon. Pour tester la sécurité du mot de passe chez un ami consentant par exemple, il faudra trouver un dictionnaire de mots français. En effet dans un dico américain vous allez trouver des mots qui ne seront sans doute pas choisis par un francophone sans compter les caractères accentués, absents des dicos anglais. On trouve aussi des dictionnaires très complets, mais payants comme ceux de Openwall (**www.openwall.com/wordlists**). Pour tester l'appli, nous avons trouvé un petit dico français au format TXT disponible à cette adresse : **www.gwicks.net/dictionaries.htm**. Libre à vous de chercher plus avant et de nous faire part de vos découvertes !

ATTENTION AUX FAILLES DES ROUTEURS

Si vous utilisez une box (une belle exception française !), ce problème ne vous concerne pas puisque les FAI mettent automatiquement à jour leur matériel. Par contre, si vous utilisez un routeur, attention ! Des failles internes à certains modèles permettent aux hackers d'accéder à votre réseau sans effort ! Pour éviter ce genre de déconvenue, il est conseillé de mettre à jour manuellement votre routeur en consultant la page du fabricant. Nous y reviendrons dans un prochain numéro !

UTILISATION ET OPTIMISATION DE WIBR+

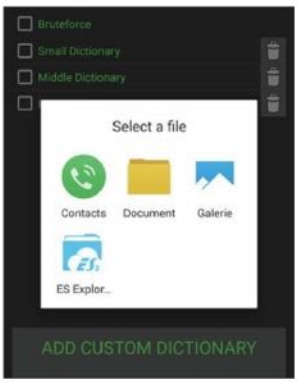
01 › LA CIBLE

L'appli n'est pas dans le PlayStore, il faudra la télécharger en suivant notre lien (et uniquement ce dernier). Vous devrez aussi autoriser l'installation des sources inconnues dans les paramètres. Si vous avez un antivirus, il va peut-être se manifester. Faites-lui comprendre que tout va

bien. Appuyez sur **ADD NETWORK** et choisissez le SSID du réseau que vous voulez tester.

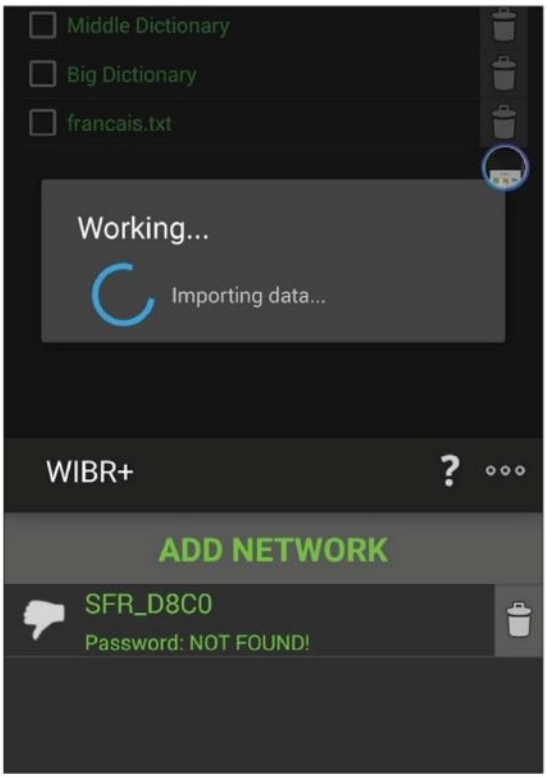
02 › ATTAQUE DICTIONNAIRE

Nous allons commencer par la méthode par dictionnaire réputée plus rapide. Vous allez voir que l'appli dispose de 3 dicos comportant plus ou moins de mots de passe enregistrés. Nous n'allons pas les utiliser, car ils ne sont pas adaptés aux utilisateurs francophones. Faites **ADD CUSTOM DICTIONNARY** et cherchez votre dictionnaire (voir notre encadré) au format TXT dans votre téléphone avec votre explorateur de fichiers. Téléchargez-en un si vous n'en avez pas.



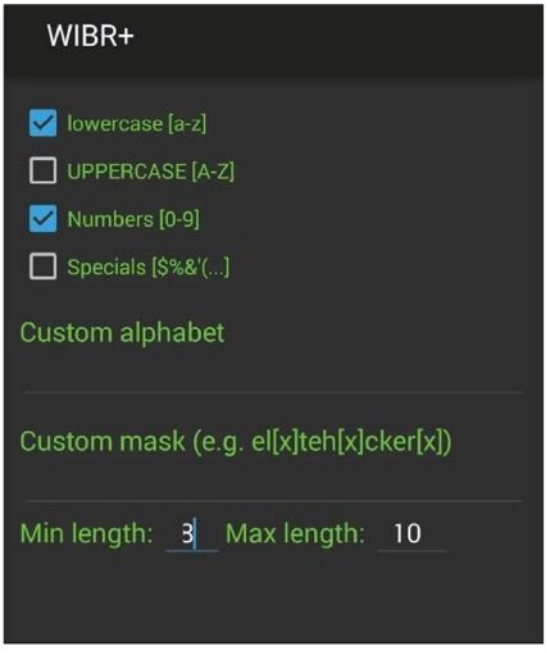
03 › LE FICHIER DICTIONNAIRE

Notez que ce fichier TXT devra comporter les sésames à raison de un par ligne et que plus vous aurez de mots de passe dans le fichier et plus il faudra attendre que l'appli les intègre (**Importing Data**). Au bout du processus, vous verrez que votre dico sera dans la liste avec les autres. Cliquez sur la case correspondante et faites **ADD TO QUEUE**. Malheureusement, nous avons fait chou blanc. Le mot de passe ne se trouve pas dans le fichier.



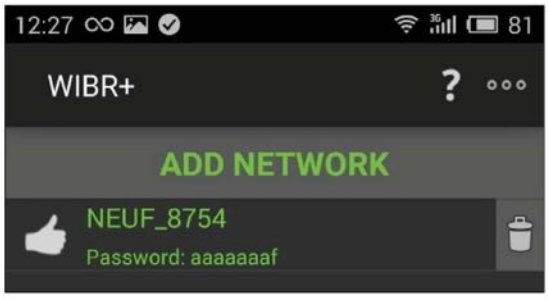
04 › ATTAQUE BRUTEFORCE

Tentons alors la méthode par force brute. Resélectionnez le SSID cible, cochez la case **Bruteforce** et choisissez **CONFIGURE BRUTEFORCE**. Ici vous pourrez choisir les jeux de caractères, la longueur du mot de passe, ajouter un autre alphabet ou mettre un «masque». Cette option vous servira si vous avez une partie du mot de passe. Par exemple si vous savez que le sésame commence par **admin** et qu'il y a deux chiffres après, vous pouvez écrire **admin[x][x]**. L'appli essaiera alors **admin00**, **admin01**, etc.



05 › UN PROCESSUS TRÈS LONG

Appuyez sur **SAVE CONFIGURATION** puis **ADD TO QUEUE** pour commencer le processus. Moins vous en savez sur le mot de passe (longueur, types de caractères, etc.) et plus la recherche va être longue. Dans notre cas, nous avons fait exprès de baisser le niveau de sécurité de notre sésame et Wibr+ a trouvé **aaaaaaaf** en quelques minutes. Pour **Fg7^mP586/*P)ç-Hjj**, sans masque et sans connaître le nombre de caractères, c'est mission impossible.

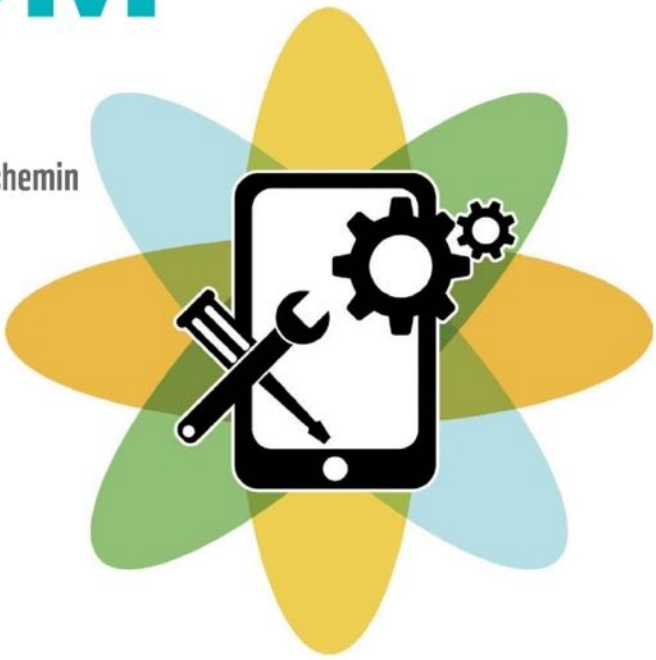


ET DU CÔTÉ DE LA POMME ?

Sur les markets alternatifs on trouve aussi des applis iOS qui permettent de cracker le WiFi. On compte notamment SpeedSSID qui va tenter de saisir le mot de passe par défaut de certains types de routeurs ou iSpeedTouch qui utilise les rainbow tables pour accélérer le processus (voir *Pirate Informatique* n°31).

PASSEZ AUX ROMS CUSTOM

Vous avez rooté votre appareil Android avec succès et installé quelques applis « root only ». Ne vous arrêtez pas en si bon chemin et changez carrément de ROM !



Vous aimez bien Windows sur votre PC, mais vous aimeriez un petit quelque chose en plus. Vous installez alors FundowsOS. C'est Windows, mais en mieux, ou en tout cas avec les fonctions que vous cherchiez. Une ROM Custom Android, c'est la même chose, un système d'exploitation alternatif, basé sur Android, mais avec plus de possibilités. L'autre avantage, c'est que les vieux modèles peuvent bénéficier de la dernière version d'Android, à laquelle ils n'ont officiellement pas le droit, tout en accédant à des options de personnalisation poussées.

DES PRÉCAUTIONS À PRENDRE

Les ROMs Custom sont basées sur la version AOSP (open source) d'Android, ce qui signifie que, de base, elles ne contiennent aucune application Google, qui ne fonctionneront pas (même le Play Store). Il faudra installer le tout à part, via le projet Open Gapps (http://opengapps.org). Vous pouvez très bien utiliser une ROM sans les Gapps, ou n'installer que la prise en charge du Play Store. Et si vous êtes à l'aise, sachez qu'il est possible de jongler entre plusieurs ROMs au gré de vos envies, via des applications (ROM Installer ou System Updater par exemple). Enfin, notez que si les mises à jour sont fréquentes, elles concernent surtout des versions en développement, potentiellement porteuses de bugs.

CHANGER DE ROM N'EST PAS PLUS COMPLIQUÉ QUE D'INSTALLER WINDOWS. ET C'EST GRATUIT !

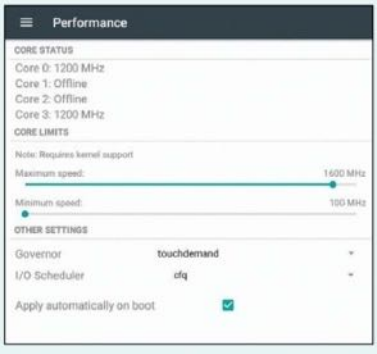
6 ROMS CUSTOM QUI VALENT LE DÉTOUR

> LineageOS

Vous connaissez sûrement LienageOS sans le savoir. Si l'on vous dit CyanogenMod, ça vous parle plus ? L'équipe de LineageOS est la même, prenant la suite du projet Cyanogen désormais arrêté. Avec plus de 80 appareils compatibles au compteur, c'est un excellent point d'entrée dans le monde des ROMs Custom. Le design est très proche d'Android «classique», mais les fonctions plus poussées, comme la gestion des permissions des applis, la customisation de la barre de statut (là où l'heure est affichée), etc. Il faudra un peu de temps pour que LineageOS arrive au même rythme de croisière que CyanogenMod, mais la communauté semble motivée.

> OmniROM

À l'origine, cette ROM a vu le jour en réaction à la «commercialisation» de CyanogenMod, et la création de l'entreprise CyanogenINC. On observe donc des similitudes avec cette dernière. Aujourd'hui, c'est une alternative solide à LineageOS, déjà parce qu'elle ne prend pas en charge les mêmes appareils, mais aussi parce qu'elle s'éloigne de LineageOS et de son envie de rester proche d'Android. Des fonctionnalités plus originales sont ainsi testées régulièrement, comme un contrôleur de performances intégré. Une ROM efficace qui ravira les amateurs de bidouille.



> CopperHead

Une curiosité qui ne fonctionne que sur les appareils Nexus (5X, 6P et 9). CopperheadOS est la ROM 100% sécurité. Après installation, c'est un peu comme si vous aviez transformé votre appareil en Blackphone. Du kernel à l'espace de stockage, en passant par les permissions des applications, tout est chiffré, verrouillé et vérifié. Toutes ces précautions peuvent avoir un impact sur les performances, ce qui empêche de diffuser plus largement la ROM sur des appareils moins puissants.

INFOS [LineageOS] Où le trouver ? [**http://lineageos.org**]
[GApps] Où le trouver ? [**http://opengapps.org**]
Difficulté : ☠☠☠

> SlimRoms

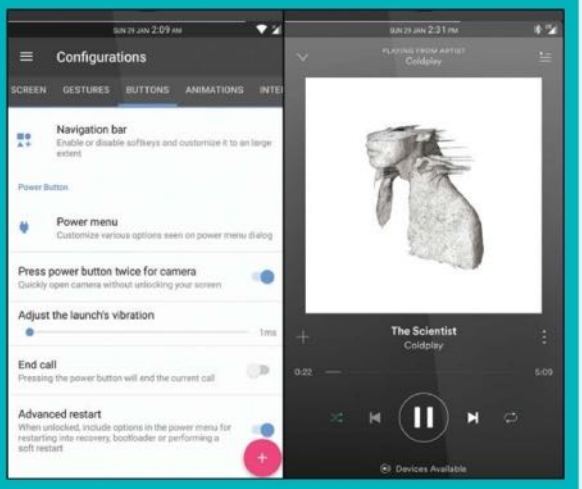
La liste des appareils supportés par SlimRom est mince (une quarantaine de modèles), mais la ROM pourra séduire certain(e)s d'entre vous par ses fonctionnalités originales, comme un menu «applications récentes» totalement repensé pour favoriser le multi-tasking ou la configuration des raccourcis accessibles par un appui long sur le bouton du lanceur d'applis. Les photographes mobiles ne sont pas en reste avec une version maison et efficace de l'application caméra. La communauté de SlimROM est active, et de nouvelles versions sont compilées chaque semaine pour la plupart des modèles.

> MIUI

Prononcée «Maï iou i», MiUI est une ROM très particulière puisqu'elle est commercialisée sur les smartphones de la marque chinoise Xiaomi. Graphiquement colorée et très proche d'iOS, elle est surtout appréciée des néo-arrivants sur Android et ex-fans d'Apple. MiUI embarque par exemple un outil permettant de gérer les notifications de vos différentes applications, ou un gestionnaire des applications qui se lancent au démarrage. Rappelez-vous que, comme sur les iPhone, MiUI ne possède pas de lanceur d'applications, ce qui peut dérouter au début. Rien ne vous empêche d'en installer un par la suite.

> Resurrection Remix

Une Rom très stable qui intègre toutes les recommandations de design de Google depuis la version Android Lollipop et son Material Design. Resurrection Remix tient son nom de ses origines. La Rom est en effet un mix de plusieurs autres Roms dont Paranoid Android, Omni, Slim et AOKP. En théorie, les développeurs ont tenu à prendre uniquement le meilleur des autres Roms, un gage de qualité. Outre le design clair et léché, Resurrection attache beaucoup d'importance à l'autonomie.



INSTALLER UNE ROM CUSTOM SUR UN APPAREIL ROOTÉ

PRATIQUE

01 › TÉLÉCHARGER LES FICHIERS

Pour l'exemple, nous allons installer **LineageOS** sur un Nexus 5X, mais la démarche reste la même pour d'autres ROMs et modèles. Téléchargez l'archive de la ROM puis la version nano (recommandé) des **GApps**, en prenant soin de cocher la bonne **Plateform** et version d'**Android** (ici 7.1 puisque la ROM est basée sur Android 7.1).

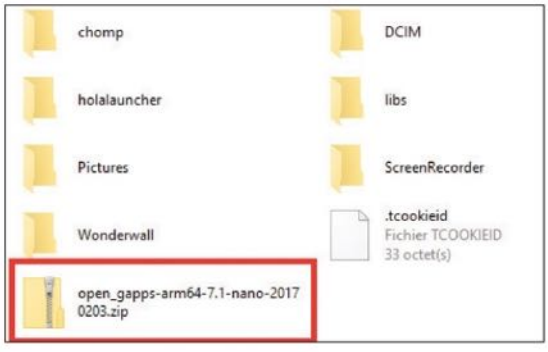
02 › INSTALLER UNE CUSTOM RECOVERY

Si, lors du root de l'appareil, vous n'avez pas

installé de Custom Recovery (une interface de démarrage spéciale), téléchargez **Official TWRP App** sur le Play Store. Ouvrez l'appli, cochez **I agree** et **Run with root permissions** puis faites **OK** et **TWRP FLASH**. Sélectionnez votre appareil dans la liste, appuyez sur la dernière version de **TWRP** et **OK**. Téléchargez l'image, revenez dans l'appli et pointez vers cette dernière avant de valider avec **Flash to Recovery** et **OK**.

03 › PRÉPARER L'APPAREIL

Branchez l'appareil au PC et placez les deux archives (la ROM et les GApps) à sa racine. Sauvegardez le contenu que vous voulez récupérer puisque l'opération va tout effacer. Idéalement, faites une sauvegarde de l'appareil avec **Titanium Backup** par exemple. Assurez-vous que la batterie est chargée à fond. Même si l'opération est assez rapide, autant être prudent.



04 › INSTALLER LA ROM

Éteignez l'appareil et redémarrez en mode **Recovery** (dans la majorité des cas : maintenez **Power** et **Volume bas**). Touchez **Wipe** et «swipez» la barre du bas. Appuyez sur **Back** puis la flèche Précédent pour aller dans **Install**. Touchez l'archive de la ROM et swipez à nouveau pour l'installer. Revenez en arrière et refaites la même chose avec les Gapps (toujours dans **Install**). Plus qu'à **Reboot** et le tour est joué ! Vous devrez reconfigurer votre appareil de zéro.

DÉCORTIQUER SON APPAREIL ANDROID

// AVEC CASTRO

Pour aller plus loin que la fiche technique de votre smartphone/tablette, rien de mieux qu'une application comme Castro qui va explorer en profondeur les caractéristiques de l'appareil. Par défaut, c'est l'onglet **Appareil** qui s'affiche à l'ouverture de l'application. Vous y trouverez, en plus du modèle, de la version de l'OS ou encore du numéro de build, les identifiants de l'appareil : numéro **IMEI** (accessible normalement en tapant *#06# sur le clavier), **Numéro de série** et **ID de l'appareil**. Accessibles après avoir touché le menu "hamburger" en haut à gauche, les autres onglets permettent d'accéder à des informations relatives à telle ou telle partie de l'appareil, comme le **CPU** (processeur), la **Batterie** ou l'**Appareil photo**. Ce dernier onglet indique notamment la distance focale du capteur photo. Pratique pour améliorer ses clichés.

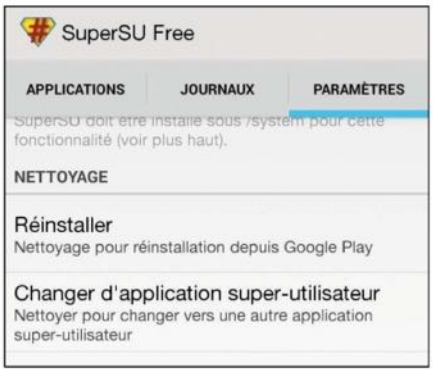
https://goo.gl/zFtJYo

RETIRER LE ROOT SUR VOTRE MOBILE

// AVEC SUPERSU

Vous souhaitez enlever le «root» de votre smartphone pour effectuer sereinement une réparation auprès de votre SAV ? Depuis l'appli SuperSu, allez dans l'onglet **Paramètres** et descendez jusqu'à la rubrique **Nettoyage**. Pour terminer, touchez **Suppression complète du root**. Voilà, vous pouvez maintenant revendre votre téléphone, le faire réparer ou supprimer un root bancal qui ne fonctionnerait pas correctement.

https://goo.gl/QDzVmm



COMMANDER SON SMARTPHONE À LA VOIX

// AVEC COMMANDR

Allumer le Wi-Fi, prendre un selfie, couper la data... autant de commandes qui peuvent être passées à la voix, sur votre téléphone, grâce à l'action combinée de Google Now et de l'application Commandr. Une fois l'application lancée, faites glisser votre doigt de la droite vers la gauche puis choisissez d'**Ouvrir les paramètres**. Activez ensuite les paramètres d'**Accessibilité** de **Commandr pour Google Now**. Dans le menu de l'appli, cochez la case **Activer interception**. Vous pouvez commencer à utiliser Commandr. Allez dans la rubrique **Commandes intégrées**. Chaque commande peut être désactivée, en basculant le bouton associé sur **Non**. Vous avez la possibilité de simplifier les commandes vocales en les éditant à l'aide du bouton crayon. Par exemple, pour lampe torche, pourquoi ne pas prononcer uniquement «**torche**» plutôt qu'**Activer la torche**? Ouvrez l'application **Recherche Google** (ou utilisez le Widget) et prononcez les termes «**Ok Google**». Prononcez la commande de votre choix une fois que le «bip» vous aura confirmé que l'appli est à l'écoute.

https://goo.gl/bXANJY

BOOTER SON PC GRÂCE À UN MOBILE

// AVEC DRIVEDROID

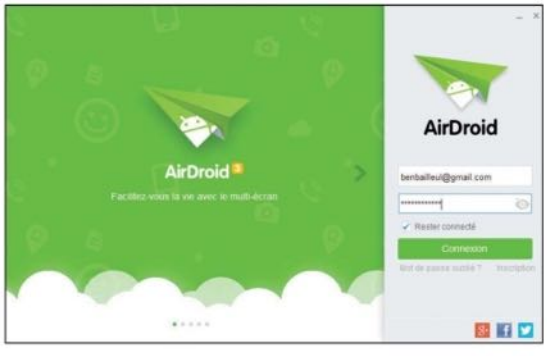
Si vous avez l'utilité de démarrer votre PC ou celui des autres depuis un LiveCD ou LiveUSB pour réparer, hacker ou changer d'OS, vous allez aimer DriveDroid. Cette appli permet de booter votre PC à partir d'une image (Windows, Linux...) stockée sur votre mobile. Cela peut se révéler pratique dans le cas où vous ne disposez pas de clef USB ou si vous voulez avoir un Kali, un Ubuntu ou un Hiren's Boot CD sous la main, quelle que soit la circonstance. Sélectionnez l'ISO à monter, branchez le câble USB entre votre smartphone et votre PC et c'est parti ! Pour la version iOS, il faudra un appareil jailbreaké et installer l'appli depuis **http://apk4ios.com**.

https://goo.gl/7FUYlU

ACCÉDER À VOTRE SMARTPHONE À DISTANCE

// AVEC AIRDROID

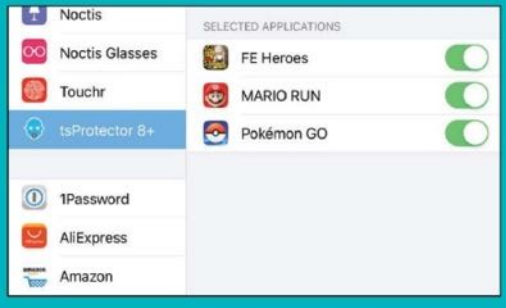
AirDroid est une application qui une fois installée sur votre appareil Android permet d'y avoir accès depuis un PC ou un Mac. Vous pourrez donc accéder à vos SMS et y répondre, transférer vos fichiers, écouter votre musique et accéder aux notifications. Vous pouvez utiliser l'interface Web ou le logiciel. Entrez les identifiants que vous vous êtes choisis auparavant et autorisez le programme à passer au travers de votre pare-feu. Bienvenu dans AirDroid! D'ici, vous pouvez ajouter des amis et envoyer des fichiers de toutes tailles, streamer du contenu multimédia, répondre à vos appels ou faire fonctionner l'appareil photo.



https://goo.gl/465MfD

MASQUER LE JAILBREAK

// AVEC TSPROTECTOR 8+



Vous n'arrivez pas à faire fonctionner Mario Run, Pokémon Go ou une autre application sur votre iPhone? C'est sans doute parce que certaines compagnies refusent de placer leur bébé dans un iPhone jailbreaké! Peur de la triche, du piratage? Pour cacher le jailbreak de votre iOS, il vous faudra simplement l'application tsProtector 8+ que vous trouverez dans le dépôt BigBoss de Cydia. Lancez l'appli récalcitrante, allez dans les paramètres de tsProtector et activez l'appli en question dans la **BlackList**. Attention, cette appli n'est pas encore compatible avec les dernières versions d'iOS.

GÉRER L'ACCÈS ROOT DE SES APPLIS

// AVEC ROOTCLOACK PLUS

Avec RootCloack Plus, vous décidez à quelles applications vous accordez les droits super-utilisateur. Pratique, sachant que certaines applis fonctionnent mal sur les mobiles rootés. Utilisez le + pour choisir les applications qui ne doivent plus accéder à ce type de droits. Attention, en fonction de votre version d'Android il faudra installer d'autres applis ou librairies : lisez bien les instructions ! RootCloak ne fonctionnera pas avec des appareils qui ont plus d'un compte utilisateur.

https://goo.gl/ohCL44

CRÉER DES RACCOURCIS POUR REDÉMARRER

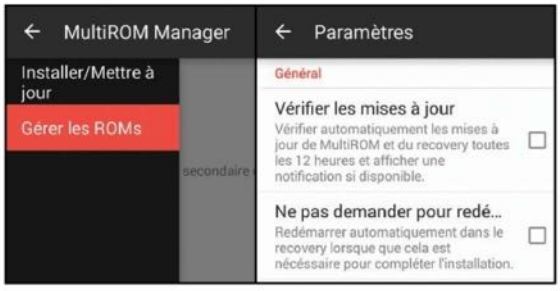
// AVEC QUICK REBOOT

Cette appli sert à définir des raccourcis permettant par exemple de redémarrer rapidement en mode Recovery ou d'accéder directement au bootloader. Ouvrez l'application puis faites votre choix parmi le Reboot classique, le Recovery, le Bootloader... Notez qu'il vous faut Autoriser la requête demandant les droits super-utilisateur pour l'application pour lancer le redémarrage selon le mode choisi.

https://goo.gl/A4ZiWO

CHANGER DE ROM CUSTOM RAPIDEMENT

// AVEC MULTIROM MANAGER



Cette appli vous aide à switcher facilement de ROM Custom (voir page 34). Vérifiez que votre appareil est compatible en vous rendant sur la fiche présentant l'appli, sur le Play Store. Il vous suffit ensuite de disposer, sur votre appareil, du fichier zip de la ROM à installer. Installez autant de ROMs que vous le souhaitez puis redémarrez, grâce à MultiROM Manager (depuis **Gérer les ROMs**), sur celle que vous voulez utiliser.

https://goo.gl/1QRqiQ

DÉBLOQUER LA 3G/4G

// AVEC 3G UNRESTRICTOR

3G Unrestrictor fait croire aux applications que l'utilisateur esten Wi-Fi alors que son appareil est connecté sur le réseau «data» en 3G/4G. Le but est évidemment de pouvoir jouer à des jeux qui nécessitent le Wi-Fi ou encore de télécharger des applications de plus 100 Mo depuis l'App Store. Pratique. Pour en profiter, il faudra jailbreaker votre appareil et acheter l'application sur Cydia pour 4 dollars.

SIMULER DES TOUCHES CASSÉES DE VOTRE SMARTPHONE

// avec Button Savior

Vos touches tactiles ou physiques indispensables (Home, retour et multitâches) ne répondent plus ? Essayez l'appli **Button Savior** . Une fois l'application installée et ouverte, une barre d'actions apparaît sur votre droite. Cette dernière contient les fameuses commandes indispensables. Plus besoin de racheter un smartphone !

https://goo.gl/PEKFsW

CHARGER LES APPLICATIONS PLUS RAPIDEMENT

// avec SD Booster

Android utilise un système de cache pour stocker les fichiers les plus utilisés afin de gagner du temps. En augmentant la taille du cache pour stocker plus de fichiers, vous accélérez le chargement des applis. **SD Booster** modifie l'espace alloué au cache. Dans le champ **KO**, renseignez une valeur de cache comprise entre **128** ou **8192** (selon la RAM de votre mobile). Essayez ensuite de lancer plus d'applications en même temps et voir ce qu'il se passe.

https://goo.gl/DDZFFR

VÉRIFIER QUE CE TÉLÉPHONE N'A PAS ÉTÉ VOLÉ

// avec Coolify

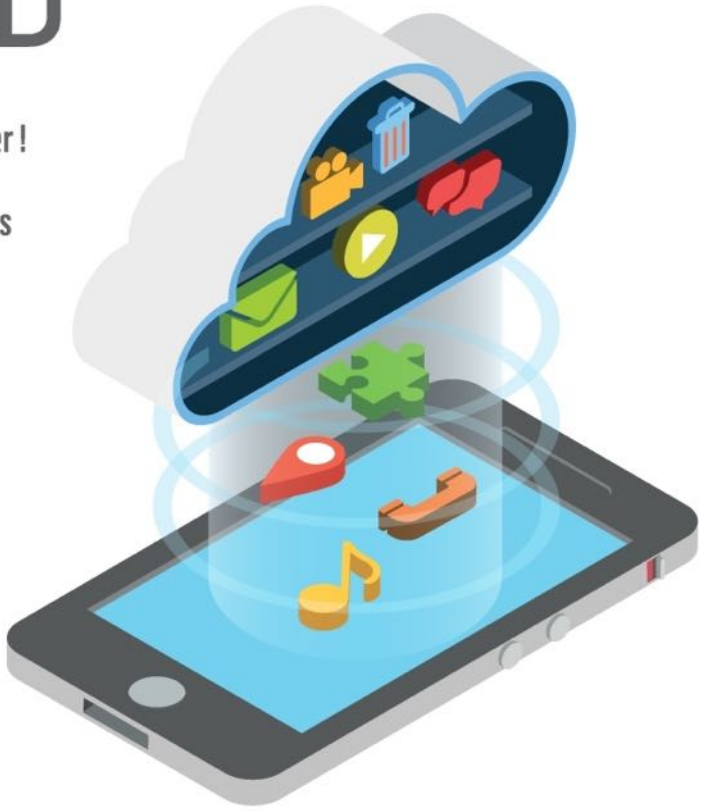
Si votre appareil chauffe de manière exagérée, rendez-vous sur le Play Store à la recherche de Coolify (pour la version iOS, il vous faudra un téléphone jailbreaké et l'installer depuis http://apk4ios.com). Pressez **Turn On Normal Temp Protection**. L'appli tente de maintenir la température du processeur à un niveau acceptable. Depuis les paramètres (**Settings**), choisissez de lancer l'appli au démarrage du système (**Set on boot**). Plus besoin de lancer l'appli manuellement.

https://goo.gl/MWUQyC

PROTECTION

SAUVEGARDEZ VOTRE APPAREIL ANDROID

Avant de rooter, il faut sauvegarder ! On vous l'a dit assez souvent pour que ce soit bien ancré, alors voyons maintenant comment faire.



Applications, photos, vidéos, musiques, mais aussi sauvegardes de jeux, il y a pas mal de choses à sauvegarder avant de rooter son smartphone. Pour rappel : la démarche efface tout et vous oblige à reconfigurer l'appareil comme si vous l'aviez allumé pour la première fois. Pour les photos ou vidéos, vous vous dites qu'il suffit de relier appareil et PC via un câble et d'opérer un simple transfert. Vous avez raison, mais il y a plus simple et plus complet : tout sauver dans le Cloud via votre compte Google, sachant que par défaut, la fonction est activée sur tous les smartphones (à vérifier dans **Paramètres > Sauvegarder et réinitialisation**). Elle s'occupe aussi de vos contacts, agendas et mails enregistrés sur Gmail, Agenda Google, etc.

UN GAIN DE TEMPS ET D'ESPACE

Pour cela, il faut accepter d'installer quelques applications Google et de jouer l e jeu du Cloud : toutes les sauvegardes vont se faire dans les nuages. L'avantage, c'est que vous libérez de l'espace et que vous pouvez tout retrouver à partir de votre compte. Le désavantage, c'est que vous confiez vos fichiers à des services externes. Vous pouvez aussi tout faire en local, mais c'est plus fastidieux : utilisez **ES Explorateur de fichiers** pour transformer vos applis en APK, sauvegardez vos SMS/MMS avec **SMS Backup & Restore** et les données d'applications avec **Helium** (cf. tutoriel page 44). À vous de voir quelle méthode vous préférez !

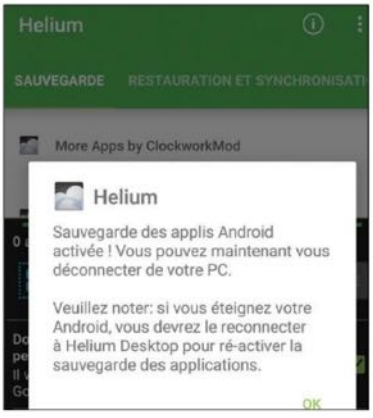
INFOS [Helium]
Où le trouver ? [**www.clockworkmod.com/carbon**]
Difficulté : ☠☠☠

SAUVEGARDER LES DONNÉES D'APPLICATIONS AVEC HELIUM

PRATIQUE

01 › LES OUTILS

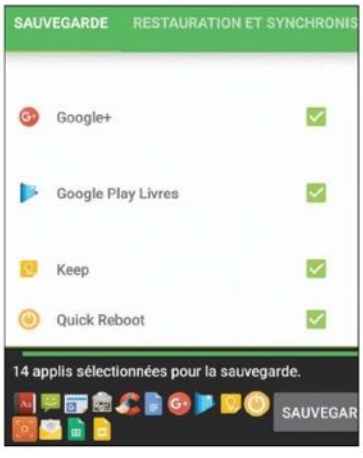
Helium sert à sauvegarder en local les données d'applis en tout genre que Google ne gère pas (réseaux sociaux, banque, messagerie...).



Installez Helium sur le smartphone depuis le Play Store. Sur le site d'Helium, récupérez le programme de votre choix (ici: l'extension Chrome). Branchez le mobile au PC puis ouvrez l'appli et le programme Helium. Touchez **OK** dans l'appli et attendez la confirmation d'activation.

02 › LA SAUVEGARDE

Sur le smartphone, cochez les cases des applications dont vous voulez sauvegarder les données. Touchez la barre verte et faites-la glisser vers le haut ou le bas pour afficher/masquer plus d'options, comme Tout sélectionner. Une fois vos choix effectués, appuyez sur Sauvegarde puis Stockage Interne (la sauvegarde sur le Cloud nécessite la version payante d'Helium).



03 › LA RESTAURATION

Sur le PC, explorez le mobile et copiez le dossier **carbon**, puisqu'il sera perdu lors d'un root par exemple. Il faudra alors réinstaller l'application Helium, placer le dossier **carbon** à la racine du smartphone, puis ouvrir l'appli, aller dans **Restauration et synchronisation > Stockage Interne**, cocher les cases souhaitées et valider avec **Restaurer**.

ET SI L'ON EST DÉJÀ ROOTÉ ?

Si vous avez les droits root, c'est beaucoup plus simple. Il est possible de faire un backup complet de son appareil via **TWRP** (ou une autre recovery custom). Redémarrez en mode **Recovery** et allez dans **Backup**. Cochez ce qu'il faut conserver et «swipez».
La sauvegarde se récupère dans **Restore** : touchez l'archive et swipez.

TOUT SAUVEGARDER AVEC GOOGLE

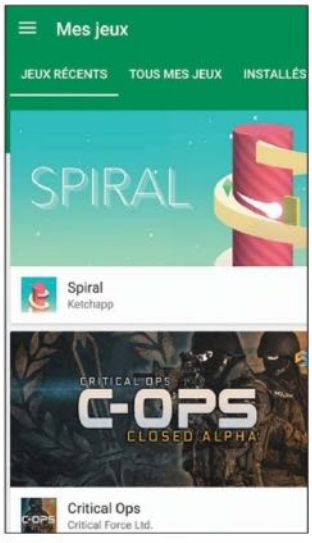
PRATIQUE

01› VOS APPLICATIONS

Toutes les applications que vous installez sont sauvegardées sur votre compte Google. Quand vous vous connectez sur une autre tablette avec ce compte (ou la même après réinitialisation), elles sont installées à nouveau. S'il en manque, pas de panique : ouvrez le **Google Play Store** puis le menu hamburger (les 3 traits parallèles) et touchez **Mes applications> Toutes**. La liste est complète.

02› VOS SAUVEGARDES DE JEUX

Retrouvez son jeu, c'est bien. Le reprendre là où l'on en était, c'est mieux. La plupart des jeux récents intègrent **Google Play Jeux**, ce qui permet, avec votre autorisation, de conserver une sauvegarde de votre avancée dans le Cloud. Si le jeu n'est pas compatible avec Google Play Jeux, vérifiez s'il propose un code en guise de sauvegarde. Sinon, utilisez une application comme **Hélium** (cf. page précédente).



03› VOS PHOTOS ET VIDÉOS

Non seulement **Google Photos** permet de sauvegarder clichés et vidéos dans le Cloud, assurant leur récupération, mais il peut aussi le faire sans aucune limite de stockage ! Pour cela, allez dans les **Paramètres** de l'appli et touchez **Sauvegarder et synchroniser**. Activez la fonction puis rendez-vous dans Taille d'importation pour choisir **Haute qualité**. Les photos et vidéos sont alors limitées à 16 Mégapixels, ce qui est largement suffisant pour un usage classique.

04› VOS MUSIQUES

L'application Google Musique est là pour sauvegarder toutes vos chansons dans le Cloud. Inutile de souscrire à l'abonnement mensuel : dans sa version gratuite, l'appli permet d'enregistrer jusqu'à 50 000 titres ! Seul «inconvénient» : rapatrier vos morceaux se fait depuis votre PC, via l'outil **Music Manager** (**https://goo.gl/bbwbs**). Si vos morceaux sont sur votre smartphone, il faudra d'abord les copier sur le PC.

PROTÉGEZ VOTRE SMARTPHONE DES MALWARES

Backdoor, ransomware, locker... Android n'est pas exempt d'attaques malveillantes. Les solutions antimalwares sont légions sur le Play Store, mais sont-elles vraiment utiles ? On fait le point.

Près de 600 millions de programmes malveillants sur Android en 2016. Un chiffre en constante augmentation, avec environ 5 nouveaux par seconde (source : AV-Test). Précisons qu'il s'agit de malwares, et pas de virus, qui est un type particulier de malware. Sur Android, on trouve des ransomwares (qui bloquent l'appareil jusqu'à paiement d'une rançon), des adwares (qui affichent des publicités non souhaitées) ou encore des spywares (qui récupèrent vos données personnelles). Un antimalware est là pour vous protéger de ces programmes fort peu sympathiques. Le problème est que dans le même temps, de nombreuses voix s'élèvent pour soutenir que les antimalwares ne servent à rien sur Android... Disons-le tout net : si votre appareil n'est pas rooté, que vous ne téléchargez

jamais d'APK, et que vous surfez uniquement sur des sites connus et sûrs, un antimalware est superflu, puisque vos comportements à risque sont proches de zéro. Si vous êtes rooté et que l'installation d'APK fait partie de votre quotidien, vous devez d'abord faire très attention à la source des applications et aux permissions qu'elles demandent. Ajouter un antimalware a du sens, une couche de sécurité supplémentaire étant toujours bonne à prendre.

GOOGLE NE ME PROTÈGE PAS ?

Toutes les applications du Google Play Store sont analysées avant publication par un système interne censé vérifier la présence de programmes malveillants. De plus, la fonction « Verify Apps » est activée par défaut sur les appareils Android, et permet de protéger l'utilisateur des applications provenant d'autres sources. À partir de là, pourquoi installer un antimalware ? Tout simplement parce que, de l'aveu même de Google dans son rapport sur la sécurité d'Android en 2015, 0,15 % des applications malveillantes proviennent du Play Store, ce qui en fait quand même presque 2 millions ! Sachant qu'il s'agit à chaque fois d'applis « légitimes » au premier abord, comme Energy Rescue, qui, sous couvert d'augmenter la durée de vie de votre batterie, volait vos SMS et contacts puis bloquait l'appareil avant de demander une rançon. Même si Google réagit vite (au bout de 4 jours pour Energy Rescue par exemple), cela laisse le temps à plusieurs centaines de milliers de personnes d'être infectées...

ANTIMALWARE, MAIS PAS QUE

Mis part quelques exceptions notables comme Avast, les applications antimalwares sont multifonctions : antivol, nettoyage de traces, verrouillage d'applications, galerie de photos privée... Même si vous ne pensez pas avoir l'utilité d'une protection contre les programmes malveillants, le côté « tout-en-un » de ce genre d'applis peut vous intéresser. La fonction antivol notamment, celle-ci étant généralement plus poussée que celle présente par défaut sur Android (le Gestionnaire d'appareils). L'un dans l'autre, pour peu que vous utilisiez une application légère et peu intrusive par défaut, comme celle présentée page suivante, vous ne perdez rien à installer un antimalware sur Android, à condition de vouloir se servir des fonctions annexes qu'il apporte. Mais n'oubliez pas une chose : la première protection contre les programmes malveillants, c'est vous.

INFOS [AhnLab V3 Mobile Security]
Où le trouver ? [**https://goo.gl/ayNnCe**]
Difficulté : ☠☠☠

LES FONCTIONNALITÉS D'AHNLAB V3

PRATIQUE

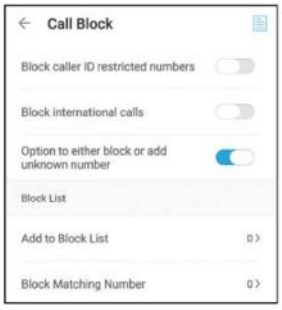
01 › NETTOYER SES TRACES

Un peu à la manière de Ccleaner,

Privacy Cleaner va chercher sur votre appareil toutes les traces potentiellement sensibles laissées par les applications. Plus que gagner de la place, il s'agit surtout d'effacer des données qu'un malware pourrait récupérer et exploiter. Cochez les cases de votre choix et validez avec **Clean**.

02 › BLOQUER LES APPELS

Si votre smartphone Android ne possède pas la version 7.0 qui l'intègre, le blocage d'appels est bien utile. **Call Block** permet de placer des numéros de téléphone indésirables en liste noire, soit manuellement, avec **Add to Block List** puis le «+», soit globalement, comme les appels qui commencent par tels ou tels chiffres, avec **Block Matching Number** et me «+». les cases de votre choix et validez avec **Clean**.



03 › L'ANTIVOL

L'antivol (**Anti-Theft**) est probablement la fonction annexe la plus intéressante. Elle permet de verrouiller, localiser, et effacer l'appareil à distance. Lors de la configuration, il faudra indiquer un numéro de confiance qui recevra des SMS d'alerte en cas de changement de carte SIM sur votre téléphone. Notez que les données effacées seront irrécupérables, AhnLab ne les conserve pas.

LES AUTRES FONCTIONS

Le scan des URL, le verrouillage d'applications et la galerie photos cachée sont des fonctionnalités payantes. Elles sont néanmoins gratuites pendant 10 jours. Les développeurs ont déjà prévenu qu'une version 4 d'AhnLab Mobile Security sortirait courant mars. Le mieux est donc d'attendre avant d'envisager de passer à la caisse.

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3€

Chez votre marchand de journaux

INFOS **[SECURE LOGIN]** Où le trouver ? [**https://goo.gl/xEVnqc**]
[LOGMEIN] Où le trouver ? [Android > **https://goo.gl/xDiAZH**] [iOS > **https://goo.gl/FY36wS**]
Difficulté :

AUTHENTIFICATION SÉCURISÉE AVEC FIREFOX

Vous êtes un inconditionnel de Firefox sur PC/Mac et vous voudriez automatiser les authentifications et profiter de vos mots de passe sur votre appareil mobile (iOS & Android) ? En utilisant les extensions que nous vous conseillons et en actionnant la synchronisation, vous allez gagner du temps tout en étant protégé des pirates.

Vous utilisez la mémorisation des mots de passe de Firefox sur votre PC ? C'est une bonne idée tant que vous utilisez un mot de passe Windows pour blinder votre session et le mot de passe principal du navigateur pour protéger tous les autres. Avec l'extension Secure Login en plus, vous allez vous simplifier la vie. Cette dernière permet d'améliorer les fonctionnalités du gestionnaire de mots de passe de Firefox. Une fois installée, vous pourrez vous authentifier sur un site en un clic, même si vous disposez de plusieurs comptes. Il est possible de voir si les identifiants sont enregistrés avec un code couleur. D'ailleurs, Secure Login fait aussi office de protection contre le phishing puisque les identifiants ne se chargeront pas s'il s'agit d'un site frauduleux. Pour synchroniser vos identifiants/mots de passe, vous pouvez compter sur l'option de synchronisation de Firefox puisque cette dernière fonctionne très bien sur mobile ou sur PC.

POURQUOI NOUS PRÉFÉRONS FIREFOX ?

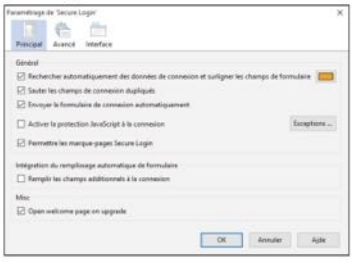
Mozilla Firefox est le deuxième navigateur le plus populaire en France avec pas loin de 23% de parts de marché. C'est loin derrière Google et son Chrome (34%), mais mieux que Microsoft et son Explorer/Edge (moins de 20%). Pourquoi nous préférons Firefox à la rédaction ? Parce qu'il ne vient pas d'un grand groupe américain, mais d'une fondation à but non lucratif.

MOTS DE PASSE FIREFOX : ENREGISTRER ET SYNCHRONISER

PRATIQUE

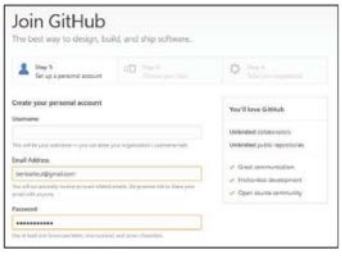
01 › LES OPTIONS

Sur le site, faites **+ Add to Firefox** puis **Installer** et enfin **Redémarrer maintenant**. Un nouveau bouton devrait apparaître dans la barre d'outils en haut à droite. Faites un clic droit dans ce dernier et choisissez **Options**. Ici, vous aurez l'onglet **Principal** qui vous permettra de paramétrer un code couleur : si Firefox connaît les identifiants, vous verrez les champs des formulaires entourés d'orange par exemple (pratique si vous avez par exemple oublié que vous aviez déjà un compte).



02 › AUTHENTIFICATION EN UN CLIC !

Faites le test et lancez une page ou un service Internet sur lequel vous êtes enregistré. Sur la page de connexion, faites un clic sur le bouton ou utilisez le raccourci clavier que vous avez paramétré. Et voilà, vous êtes loggé ! Si vous avez activé l'option des marque-pages Secure Login, faites un clic droit dans le bouton et enregistrez votre page comme un favori.

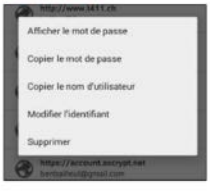


03 › SYNCHRONISATION VERS LES MOBILES

Si vous utilisez Firefox sur votre mobile (iOS et Android) vous pouvez utiliser la méthode de synchronisation. Sur votre PC, cliquez sur les trois barres horizontales en haut à droite et faites **Se connecter à Sync**. Créez un compte et choisissez les éléments à synchroniser : onglets ouverts, mots de passe, historique, modules complémentaires, etc.

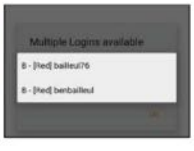
04 › TOUS VOS FIREFOX À L'UNISSON

Validez votre inscription depuis votre client de messagerie puis ouvrez la version Firefox sur votre mobile. Allez à l'onglet **Historique**, faites **Démarrer** et entrez les identifiants de connexion que vous venez d'entrer. Bravo, tous vos identifiants et mots de passe sont transférés sur votre nouvel appareil. Sur votre mobile, allez dans **Outils** > **Identifiants** pour les voir, domaine par domaine. Vous pourrez revenir ensuite dans les options pour gérer les appareils connectés dans la partie **Sync**.



05 › LOG ME IN = SECURE LOGIN

Maintenant que vos différents Firefox sont synchronisés, sachez que vous pouvez utiliser l'extension Log Me In pour mobile. Cette dernière agira exactement de la même manière que Secure Login (qui n'existe pas en version mobile pour le moment). Lorsque vous êtes sur un site connu et sur lequel vous avez un compte, une petite icône en forme de clé va apparaître. Il suffit de cliquer dessus pour se logger automatiquement. Cela fonctionne aussi si vous avez plusieurs comptes sur un même site.



SURVEILLER L'ACCÈS INTERNET DE SES APPLIS

// avec Fire sans Root

Comme sur votre bon vieux PC, l'utilisation d'un pare-feu se révèle judicieuse sur un appareil mobile Android. Firewall sans root se charge de contrôler l'accès au Web que requièrent, à juste titre ou non, certaines applications. Elle vous prévient dès que l'une des applications installées sur votre appareil tente de se connecter à Internet. À vous d'**Autoriser** ces dernières ou de les **Refuser** suivant la nature de l'appli. Avouez qu'une lampe-torche qui accède au Web, c'est louche.

https://goo.gl/gtjR6m

LOCALISER SON SMARTPHONE DÉROBÉ

// avec Android Device Manager

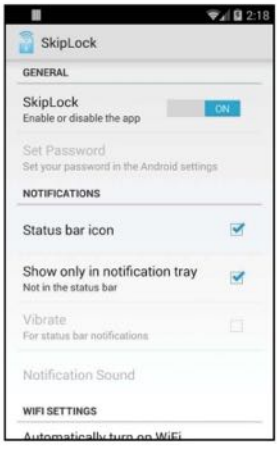
À la manière d'Avast Anti-Theft, Google propose une solution native de contrôle à distance de son appareil. Android Device Manager dispose d'une interface Web, accessible avec votre compte Google (le même que celui de votre téléphone perdu). Une fois connecté, vous avez la possibilité de localiser votre appareil, de le **Verrouiller**, de le **Faire Sonner** ou encore d'en **Effacer** tout le contenu.

https://goo.gl/XtZfGc

DÉVERROUILLER SON MOBILE SUIVANT SA POSITION

// avec SkipLock

Vous en avez marre de déverrouiller votre mobile avec un code ou un schéma lorsque vous êtes dans un lieu de confiance ? Installez SkipLock. L'appli vous aide à définir le mode de déverrouillage qui doit s'appliquer suivant votre position. Pour résumer, un mot de passe vous sera demandé lorsque vous utiliserez votre smartphone préféré dans la rue. En revanche, vous pourrez choisir de désactiver ce mot de passe (code PIN dans l'appli), lorsque vous êtes connecté à un réseau Wi-Fi. L'appli existe aussi pour les iPhones jailbreakés. Elle se trouve dans le dépôt BigBoss de Cydia...



https://goo.gl/BwVfn9

SCANNER SON RÉSEAU WI-FI

// AVEC FING NETWORK SCANNER

Network Discovery vous donne la possibilité de repérer tous les appareils branchés sur votre réseau Wi-Fi. Pratique pour identifier les éventuels « squatteurs ». Une fois l'application lancée, appuyez sur **My Network** pour effectuer le scan réseau. L'adresse IP de chaque appareil connecté sera renseignée, ainsi que la marque de ce dernier. À vous ensuite d'identifier la source de vos problèmes de connexion. L'appli propose aussi différents outils d'audit réseaux. A vous de découvrir toutes les fonctionnalités.

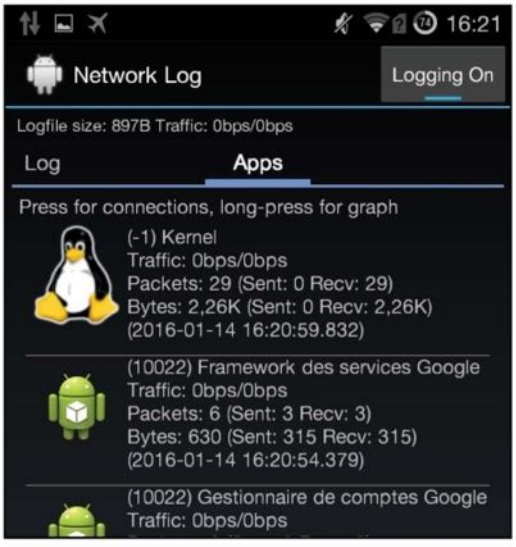
www.fing.io

SURVEILLER SON RÉSEAU WI-FI

// AVEC NETWORK LOG

Cette appli permet de monitorer en temps réel les autres applis d'un appareil Android. Il s'agit de savoir quelle appli se connecte quand, via quel réseau et pourquoi. Network Log est très détaillé, on peut même connaître l'IP de destination, le nombre de paquets de données envoyés, la vitesse de transmission... pour contrôler d'où les fuites de données mobiles peuvent provenir.

https://goo.gl/ZdrnZE



SCANNER SON APPAREIL MOBILE

// AVEC CM SECURITY

En plus d'adopter les bons gestes (contrôler d'où proviennent vos applications, mettre à jour régulièrement ces dernières...), l'usage d'un antivirus est recommandé. CM Security est gratuit, complet et très léger. Il corrige les vulnérabilités du système et analyse les applis, les mises à jour, les systèmes de fichiers afin d'assurer la sécurité de votre appareil. Faites **Analyser** pour lancer la détection de malwares. Une fois les menaces identifiées, choisissez de **Tout résoudre**.

https://goo.gl/ZqPSAM

RÉCUPÉRER DES FICHIERS EFFACÉS PAR ERREUR

// AVEC DISKDIGGER PHOTO RECOVERY

Vous avez effacé des photos par erreur ? DiskDigger Photo Recovery, vous aide à les récupérer. Accordez les droits super utilisateur si vous les avez et sélectionnez la mémoire à scanner. Appuyez sur **Start Basic Photo Scan**. Plus qu'à choisir parmi celles qui s'affichent. La version payante de l'appli gère plus de types de fichiers (musiques, vidéos, etc.)

https://goo.gl/QPCPuD

VÉRIFIER QUE CE TÉLÉPHONE N'A PAS ÉTÉ VOLÉ

// AVEC SPIDEROAKONE

SpiderOakONE propose une solution de cloud sur ordinateur et mobile avec une technologie de chiffrement bout-à-bout (aucune clé ne transite sur le réseau et donc ne pourra être interceptée.) L'application permet d'accéder et d'afficher toutes vos données sauvegardées sur l'ensemble de vos périphériques, d'envoyer un fichier à quiconque en créant un lien de partage, de sauvegarder du contenu ou de synchroniser vos différents appareils.

https://spideroak.com

PARTAGER SÉCURISÉ

// 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-détruira*». 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. Une sorte de Snapchat fonctionnant avec tous les types de fichiers...

https://digify.com

SE DÉBARRASSER DES CHEVAUX DE TROIE

// AVEC STUBBORN TROJAN KILLER

Vous pensez que votre tablette a été infectée par un trojan, ou cheval de Troie ? Ces petits programmes très difficiles à identifier et qui peuvent vite faire des ravages sur l'appareil ? Utilisez l'application Stubborn Trojan Killer. Une fois ouverte, touchez **Scan** et, si une infection est détectée, appuyez sur **Kill** pour l'éliminer directement.

https://goo.gl/iVhqbM

CHEZ VOTRE MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

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

+ CD GRATUIT PACK 100% PIRATE

ANONYMAT

TOR SUR MOBILE : C'EST POSSIBLE !

Vous connaissez Tor sur PC ? Ce système de routing permet de masquer sa position, son identité et le type de données échangées. Idéal pour contourner les pirates et les espions, le duo Orbot/Orfox va vous fournir une IP d'emprunt et améliorer la protection de votre vie privée.

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'informations sur son successeur et son prédécesseur. Pour parfaire la sécurité, il convient néanmoins d'utiliser un navigateur qui ne trahira pas votre connexion.

ORFOX + ORBOT

L'appli Orfox est un simple navigateur dérivé de Firefox qui n'enregistre pas l'historique de navigation et permet de brouiller les pistes (en faisant croire que vous surfez d'un autre type d'appareil), contourne les pare-feu (bureau, école, etc.) et les géolocalisations, mais ce dernier à besoin d'Orbot pour fonctionner. Comme son alter ego sur PC, Orbot autorise le Protocol obfuscation. Cette option (dans Bridge), va permettre de masquer le protocole de Tor au cas où il serait bloqué dans le pays où vous vous trouvez par exemple.

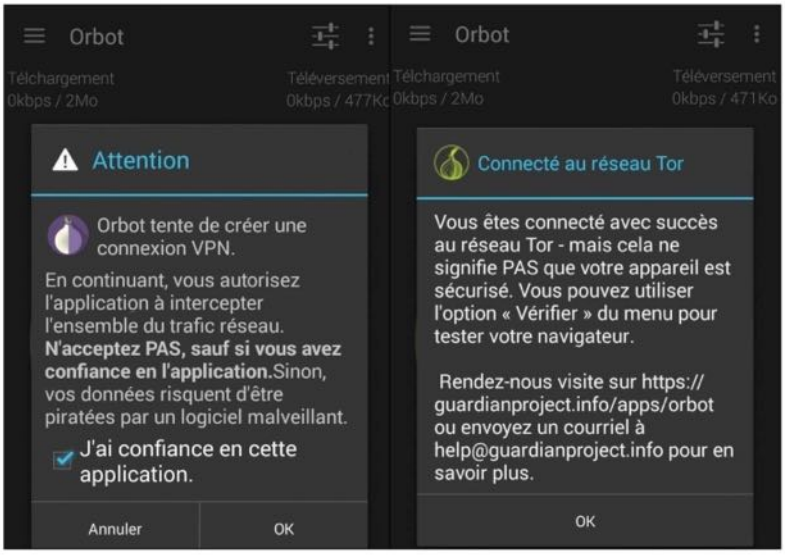
AVEC UN MOBILE ROOTÉ, C'EST MÊME L'INTÉGRALITÉ DE VOTRE TRAFIC INTERNET QUI PEUT PASSER PAR LE PROTOCOLE DE TOR...

INFOS [Orbot Proxy par Tor] Où le trouver ? [https://goo.gl/cMl1xP]
[Orfox : Tor Browser for Android] Où le trouver ? [https://goo.gl/JA7PnP]
Difficulté :

LE DUO ORBOT/ORFOX

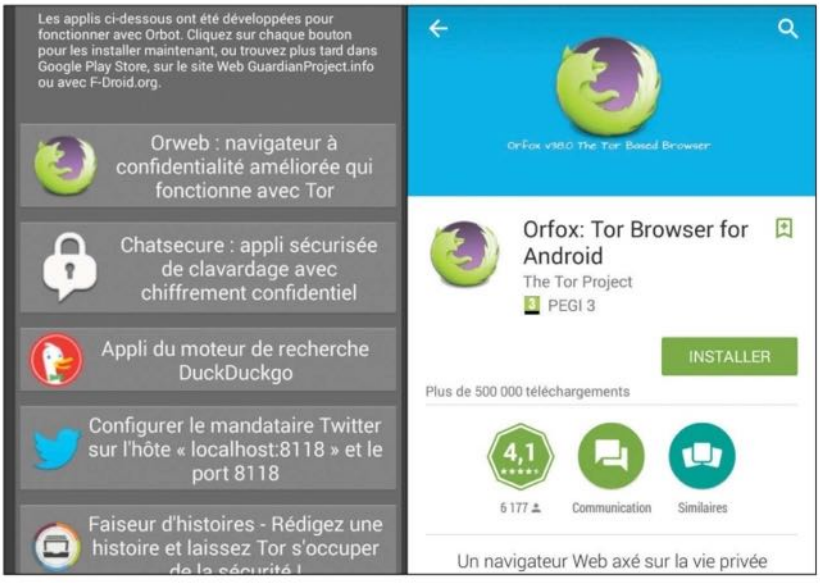
01 › LANCEMENT D'ORBOT

Commençons par installer Orbot. Lors du premier démarrage, choisissez **Appli** si vous désirez faire passer par Tor tout le trafic Internet qui émane de votre appareil. Si ce n'est pas le cas, sachez que seul le trafic du navigateur par défaut sera pris en charge. Attention Orbot est encore au stade expérimental. Cochez ensuite la case **J'ai confiance en cette application** et validez. Notez que si les textes sont en anglais vous pouvez les changer dans le menu.



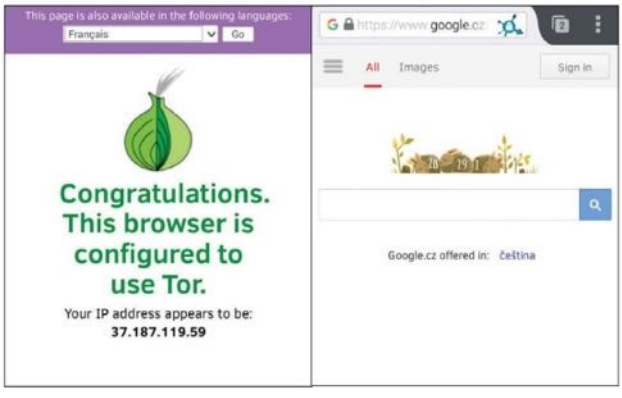
02 › INSTALLER ORFOX

Appuyez ensuite longtemps sur le bouton de démarrage puis attendez que l'appli vous informe que tout s'est bien passé (l'oignon devrait être vert). Pour vérifier que votre navigateur est bien paré pour une navigation en oignon, faites **Vérifier le navigateur**. Si vous n'avez pas de navigateur compatible, faites **Installer Orweb**. L'appli vous enverra bizarrement vers une appli similaire baptisée Orfox. Normalement Orbot devrait afficher une page vous indiquant que la navigation est sans risque.



03 › GÉRER LE TRAFIC

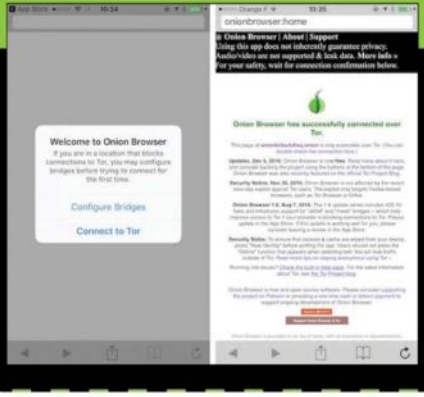
Dans les options (en haut à droite), vous pourrez choisir de démarrer automatiquement Orbot avec le téléphone et de faire passer tout le trafic par Tor. Il faudra cocher **Demander l'accès Root**, **Relayage Transparent** et **Tout passer par Tor**. Ne touchez au reste des options que si vous savez absolument ce que vous faites : **Obfs4** (protocol obfuscation) dans **Ponts**, etc. Le petit triangle en bas à droite permet même de choisir votre pays virtuel !



04 › LA NAVIGATION

Votre navigateur est prêt à démarrer ! Sur la page principale, vous pourrez paramétrer les onglets. Le premier réflexe est de se connecter à Google (mais pourquoi ne pas utiliser DuckDuckGo ou Qwant ?), mais la firme n'aime pas trop Orbot et vérifiera deux fois que le trafic ne provient pas d'un robot. Remplissez les captchas. Vous pourrez voir que dans notre exemple vous vous connectez donc depuis la République Tchèque alors que vous êtes dans votre salon.

ET DU CÔTÉ DE LA POMME ?



Autrefois vendue 1 €, l'application Onion Browser est gratuite depuis ce début d'année 2017. À cause des limitations imposées par Apple, il manque des fonctionnalités par rapport aux versions Android et PC (pas de HTTPS Everywhere ou de prise en charge d'onglets). Heureusement, les possesseurs d'appareils jailbreakés (voir page 10) disposent d'une alternative dans Cydia. Il faudra juste installer le dépôt BigBoss pour l'obtenir...
Lien : **https://goo.gl/HIhzDh**

CONVERSATION GSM CHIFFRÉE : UN SIGNAL FORT !

Open source et gratuit, Signal Private Messenger est une application permettant de sécuriser vos conversations sur mobile Android ou iOS. Comme Telegram, les messages écrits sont chiffrés, mais les conversations téléphoniques aussi !

Signal Private Messenger est issue de l'application TextSecure (qui a donné naissance à SMS Secure puis Silence lorsque Open Whisper Systems a abandonné la possibilité de chiffrer les SMS). Disponible sur iOS et Android, Signal est une appli adoubée par l'ami Snowden lui-même. Gratuite, sans pub et open source, difficile de faire mieux que cette dernière. Signal propose pourtant d'activer la conversation téléphonique à la manière de WhatsApp. On note aussi la possibilité d'importer les SMS pour envoyer des textos depuis la même interface (sous Android uniquement), mais attention, ces derniers ne

seront pas chiffrés. Et c'est justement ce qui nous intéresse ici, puisque Signal propose un chiffrement de bout en bout (le chiffrement est réalisé localement sur l'appareil qui est le seul à détenir la clé privée).

UN CHIFFREMENT DE BOUT EN BOUT

Pour ce type de protection, impossible pour l'utilisateur de commencer une conversation sur un appareil (mobile) pour la finir sur un autre (ordinateur) et vice-versa puisque les clés sont sur le téléphone. Pour plus de portabilité, les développeurs de Signal ont tout de même pensé à une solution. Il faudra passer par une extension du navigateur Chrome que l'on associera au téléphone pour profiter de bout en bout sur votre PC/Mac (voir notre prise en main).

	Signal
Chiffrement	Curve25519 + AES 256 bits et HMAC-SHA256
SMS	Oui (peut remplacer l'appli SMS par défaut sous Android, mais sans chiffrement)
Appel téléphonique chiffré	Oui
Message vidéo chiffré	Oui
Utilisation du WiFi et de la 3G/4G	Oui
Pièces jointes chiffrées	Oui
Disponible sur ordinateur	Oui pour Android et iOS, mais il faudra l'extension Chrome sur PC ou Mac et une petite manipulation (voir plus loin)
Version en ligne	Non
Autodestruction des messages	Oui, au bout d'un certain nombre de messages (chiffre défini par l'utilisateur)

POURQUOI CHIFFRER SES CONVERSATIONS ?

Depuis l'affaire Snowden, les citoyens du monde entier ont pris conscience de l'espionnage de masse dont ils étaient potentiellement victimes. Mais outre les services secrets, de nombreux autres acteurs en veulent à vos données: pirates, curieux, multinationales, police, etc. Qu'il s'agisse de documents personnels visant à usurper votre identité, de photos pour vous faire chanter, de tchats, de mots de passe ou de conversations téléphoniques, la solution consiste à tout chiffrer !

INFOS [Signal Private Messenger]

Où le trouver ? [**https://goo.gl/cMl1xP**]

Difficulté :

CONVERSATION CHIFFRÉE AVEC SIGNAL

PRATIQUE

01 › VOTRE COMPTE

Signal fonctionne comme WhatsApp : il vous faudra obligatoirement un numéro de téléphone. Ce dernier fera office d'identifiant. Notez que vous n'êtes pas obligé de renseigner le numéro de votre SIM puisque ce dernier ne sert qu'à valider votre identité. Tant que vous pouvez recevoir le code de vérification, vous pouvez mettre un autre numéro de téléphone (numéro VoIP, téléphone fixe, etc.)

02 › LE TCHAT

Si vous utilisez le même téléphone pour l'authentification et l'appli, tout est automatique. Signal vous demandera si vous préférez l'utiliser aussi comme appli SMS par défaut. Dans ce cas, les SMS ne seront pas chiffrés. Si d'autres contacts de votre liste utilisent Signal, vous les verrez aussi automatiquement. Appuyez sur le petit crayon pour choisir un interlocuteur et tchattez directement avec lui en mode chiffré (un petit cadenas doit apparaître à côté de la flèche d'envoi de message).

03 › LES OPTIONS

Vous pouvez aussi envoyer des pièces jointes et même des messages vocaux ou vidéos qui seront aussi chiffrés. Dans les paramètres (les trois petits points), il est possible de définir une durée de rétention des messages de 5 secondes à une semaine. Passé ce délai, les messages disparaîtront de votre téléphone et de celui de votre correspondant.

04 › ALLO ?

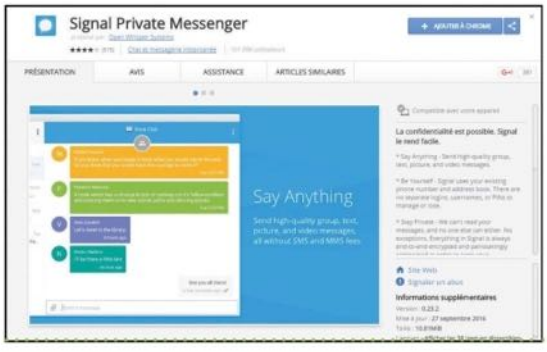
En appuyant sur le petit téléphone en haut à droite, vous allez téléphoner à votre correspondant. Le son sera chiffré et même comme cela, la qualité est au rendez-vous. Notez que deux mots aléatoires seront affichés sur l'écran au début de la conversation. Il s'agit d'une méthode pour vérifier que votre correspondant est bien celui qu'il prétend être. Donnez le premier mot, votre ami vous donne le deuxième: vous êtes alors sûr qu'une troisième personne n'usurpe pas une identité !

SYNCHRONISER SIGNAL AVEC VOTRE PC OU VOTRE MAC

PRATIQUE

01 › INSTALLATION

Depuis Google Chrome, cliquez dans les trois petits points en haut à droite puis faites **Plus d'outils >Extensions >Plus d'extensions**. Dans la barre de recherche, tapez **signal** et cliquez sur **Ajouter à Chrome> Ajouter l'application**. Faites un autre clic sur **Commencer** puis **Got It**.



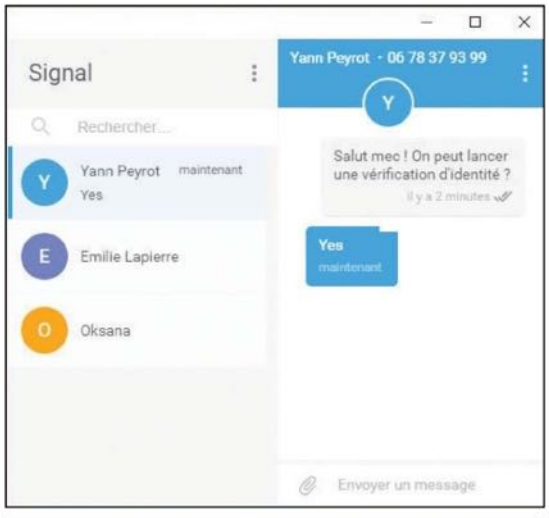
02 › SYNCHRONISATION

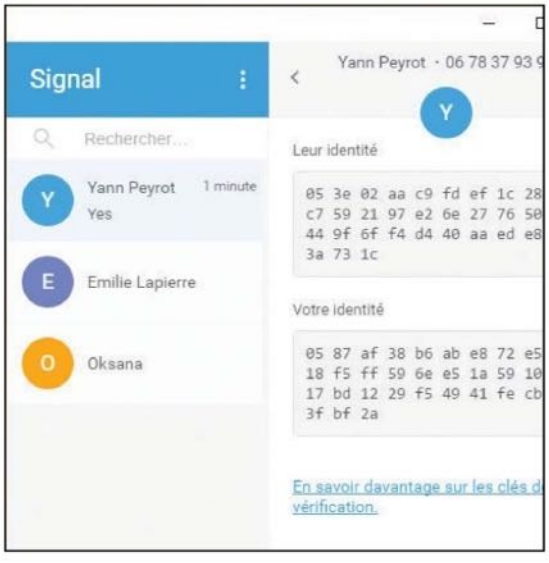
Utilisez votre smartphone pour scanner le QR Code et synchroniser l'extension avec le mobile.

Au bout de quelques secondes, vous devriez voir votre numéro de téléphone s'afficher dans une fenêtre. Validez pour voir vos contacts et converser avec eux. Les messages seront aussi contenus dans votre mobile et le chiffrement sera de bout en bout.

03 › VÉRIFIER L'IDENTITÉ DE VOTRE CORRESPONDANT

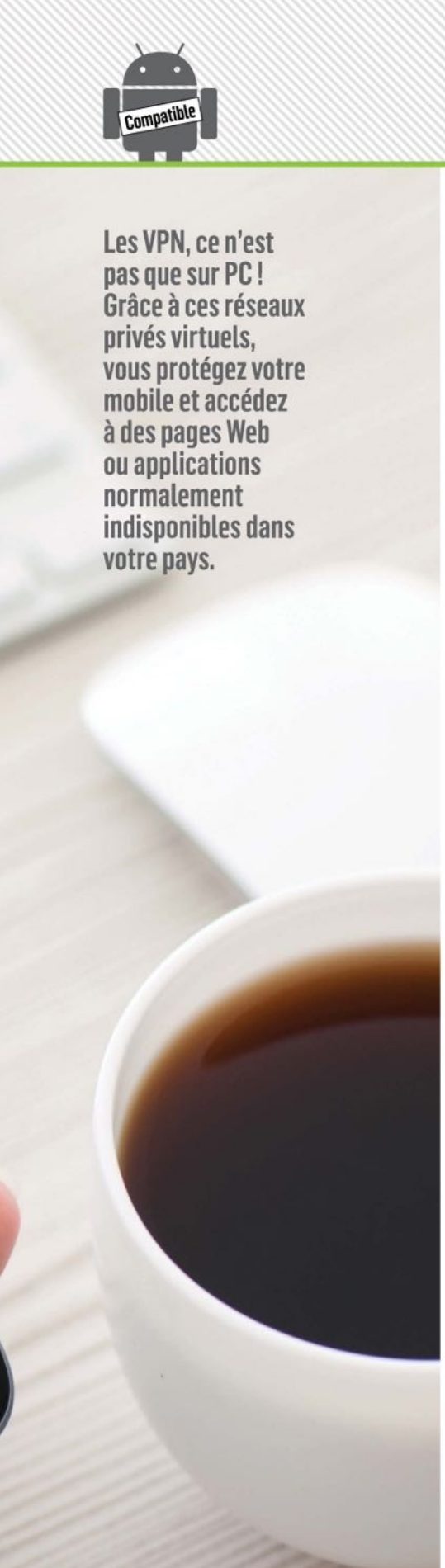
Libre à vous de vérifier l'identité de votre correspondant avec la clé publique. Sur mobile, initiez une conversation et faites **Préférences de conversation>Vérifier l'identité** tandis que sur PC, il faudra cliquer sur les trois petits point verticaux puis **Vérifier l'identité**.





SURFER ANONYMEMENT ET PROFITER D'APPLICATIONS INÉDITES

Les VPN, ce n'est pas que sur PC ! Grâce à ces réseaux privés virtuels, vous protégez votre mobile et accédez à des pages Web ou applications normalement indisponibles dans votre pays.



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. 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. Concrètement, un VPN vous permettra de surfer sur le Web de manière anonyme et sécurisée, et de télécharger des applications normalement inaccessibles en France (Hulu, Pandora, certains jeux, etc.) À l'inverse, si vous voyagez souvent à l'étranger, sachez qu'utiliser un VPN permettra d'accéder à du contenu Web géographiquement limité à la France (un service de replay d'une chaîne française par exemple).

GRATUIT, MAIS LIMITÉ

Si vous êtes familier des VPN sur PC, vous savez bien que sans passer à la caisse, ces services sont au mieux limités en vitesse et données de connexion, au pire inutilisables. Sur Android, c'est pareil. Dans la majorité des cas, un VPN gratuit vous donnera droit à 500 Mo/mois, sans choix ou avec un choix restreint de serveurs. Nous vous avons cependant déniché un VPN offrant gracieusement 10 Go/mois à ses utilisateurs, moyennant la création d'un compte gratuit : ZPN Connect. Ajoutons qu'il est compatible avec le protocole et qu'il ne conserve pas les logs de ses utilisateurs ! Vous pourrez alors vous connecter à des serveurs situés aux États-Unis, au Canada, en France (pour simplement changer d'IP), en Italie ou aux Pays-Bas. Largement de quoi couvrir l'essentiel des besoins. Notez qu'il n'est pas possible de faire du p2p via ce VPN, du moins dans la version gratuite. Enfin, si vous avez téléchargé une application indisponible en France, sachez que vous n'avez pas besoin de vous connecter au VPN pour en profiter par la suite, mais vous ne pourrez pas la mettre à jour sans.

GRÂCE AU VPN, INSTALLER PANDORA SUR UN MOBILE FRANÇAIS DEVIENT POSSIBLE.

INFOS [ZPN CONNECT]

Où le trouver ? [**https://goo.gl/zLb03l**]

Difficulté :

CONFIGURER ET UTILISER ZPN CONNECT

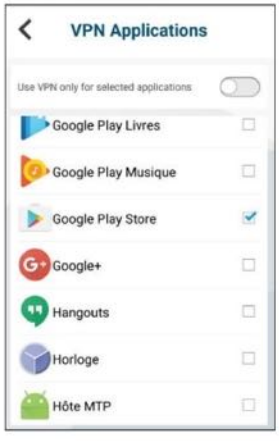
PRATIQUE

01 › CRÉER UN COMPTE

Avant d'arriver à la création de compte, vous devez indiquer si Google est disponible ou non dans votre pays, puis choisir un protocole. Si vous ne résidez pas dans un pays où le Web est contrôlé, **OpenVPN** suffit. Choisissez ensuite l'option du bas pour être invité à créer un compte gratuitement. Il faudra le valider via un lien reçu par mail, alors éviter les fausses adresses !

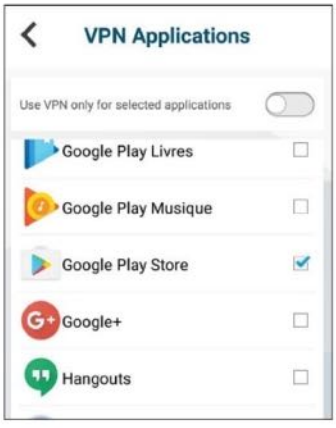
02 › CHOISIR UN SERVEUR

Avant de vous connecter, touchez les flèches bleues dans la case Location et choisissez, par exemple, **US West Coast**. Les serveurs affublés d'un premium ne sont pas sélectionnables dans la version gratuite de ZPN Connect. Basculez le curseur de **Status** vers la droite et patientez quelques secondes pour que la connexion se fasse.



03 › DÉFINIR LES APPLICATIONS

Il faut maintenant indiquer quelles applications passeront par le VPN. Touchez le menu hamburger (les 3 traits parallèles en haut à gauche) puis **Settings** et **VPN Application**. Laissez le curseur vers la gauche et cochez les applis souhaitées. Si vous voulez en cocher beaucoup, basculez le curseur vers la droite. Les applications choisies sont alors celles qui sont exclues du VPN.



04 › TÉLÉCHARGER UNE APPLICATION INDISPONIBLE

Assurez-vous d'avoir inclus le Google Play Store dans les applications profitant du VPN (cf. étape précédente). Ouvrez-le et faites une recherche tout ce qu'il y a de plus classique. L'appli de choix, ici Puzzle & Dragons, indisponible en France, apparaît dans les résultats de recherche et s'installe normalement.

ET DU CÔTÉ DE LA POMME ?

Si vous avez un appareil sous iOS, il existe des solutions de VPN même si vous n'êtes pas jailbreaké ! Allez voir les microfiches à la fin de cette rubrique pour en savoir plus !

4 VPN ALTERNATIFS GRATUITS SUR ANDROID

Vous n'êtes pas convaincu par ZPN Connect, ou n'avez pas envie de créer un compte pour en profiter ? Voici 4 VPN moins généreux en données, mais tout aussi efficaces.

VyprVPN : POUR LES DÉTAILS

VyprVPN possède moins de fonctionnalités que TunnelBear dans sa version gratuite (tout en proposant 500 Mo/mois), mais on apprécie la possibilité de monitorer la vitesse de connexion en temps réel (download et upload) et d'accéder à un journal de connexion détaillé. VyprVPN possède aussi son propre protocole, Chameleon, basé sur OpenVPN 256 bits. Il permet d'éviter le blocage des VPN ou autres limitations.

TunnelBear : POUR L'INTERFACE

Avec 500 Mo de données par mois pour l'offre gratuite, TunnelBear est un bon point d'entrée dans le monde des VPN sur Android. Ses avantages sont indéniables : interface très claire et colorée, choix entre une vingtaine de serveurs, dont les États-Unis, possibilité d'exclure certaines applis du VPN, possibilité de faire passer la connexion chiffrée pour une connexion normale... C'est simple : si vous pouvez vous contenter de 500 Mo par mois, TunnelBear est le meilleur choix.

OpenVPN Connect : POUR L'OUVERTURE

On ne pouvait pas terminer cette sélection sans parler d'un VPN open source. OpenVPN Connect (ou OpenVPN for Android, une branche basée sur le projet initial) n'est pas une appli du type « appuyez et oubliez ». C'est à vous de créer et configurer un serveur OpenVPN pour vous y connecter via l'application. Les options sont nombreuses pour qui aime fouiller dans les paramètres. À réserver aux amateurs.

SpeedVPN : POUR LA GRATUITÉ

SpeedVPN est totalement gratuit, sans limite de vitesse. Le seul inconvénient, c'est que vous êtes déconnecté automatiquement au bout d'une heure, mais rien ne vous empêche de vous reconnecter . Pas de compte à créer, vous choisissez entre les 5 serveurs disponibles, dont les USA, et vous lancez la connexion. Attention : tout téléchargement en p2p (torrent par exemple) sous SpeedVPN vous expose à un bannissement du service.

SpeedVPN est totalement gratuit, sans limite de vitesse. Le seul inconvénient, c'est que vous êtes déconnecté automatiquement au bout d'une heure, mais rien ne vous empêche de vous reconnecter . Pas de compte à créer, vous choisissez entre les 5 serveurs disponibles, dont les USA, et vous lancez la connexion. Attention : tout téléchargement en p2p (torrent par exemple) sous SpeedVPN vous expose à un bannissement du service.

INFOS [DNS CHANGER]

Où le trouver ? [**https://goo.gl/KYnDpG**]

Difficulté :

CHANGER DE DNS SUR MOBILE

Pour protéger votre vie privée, vous connaissez déjà les proxy et les VPN. Mais avez-vous pensé à changer de DNS ? On vous explique comment.

LovLe DNS (Domain Name System), c'est l'annuaire géant du Web. Chaque fois que vous voulez accéder à un site Internet, une requête est envoyée aux serveurs DNS pour récupérer l'adresse IP du serveur qui héberge ce site. Votre PC va alors pouvoir interroger ce serveur pour afficher le site sur votre écran. Dans l'absolu, on peut accéder à n'importe quel site en tapant son adresse IP plutôt que son nom de domaine. Les serveurs DNS sont bien sûr nombreux. Chaque fournisseur d'accès Internet en a un, Google en a un... Certains sont publics, voire open source, tandis que d'autres sont privés.

AU NIVEAU DE L'ANONYMAT, CHANGER DE DNS C'EST LE MINIMUM SYNDICAL.

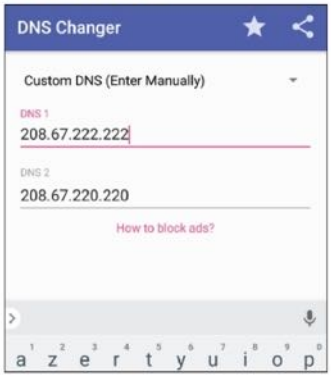
POURQUOI CHANGER DE DNS ?

L'intérêt principal, c'est l'accès à l'intégralité du Web. Un DNS sous influence filtre certains sites, ou redirige vers des sites similaires avec lesquels il a des intérêts, bref : censure Internet d'une manière ou d'une autre. La démarche est d'ailleurs invisible pour qui ne fait pas attention... Certains DNS intègrent aussi un système anti-phishing ou chiffrent l'envoi des requêtes. Sur mobile, s'il est possible de changer de DNS manuellement, il est plus simple de passer par une application pour jongler facilement entre plusieurs, de préférence open source, en quelques touches. Notez que sans root, certaines applis du genre exigent d'être connectées en Wi-Fi pour profiter de la modification. Dans la page suivante, nous utilisons DNS Changer, qui fonctionne sans root, en Wi-Fi, 3G et 4G.

MODIFIER SON DNS SUR ANDROID

PRATIQUE

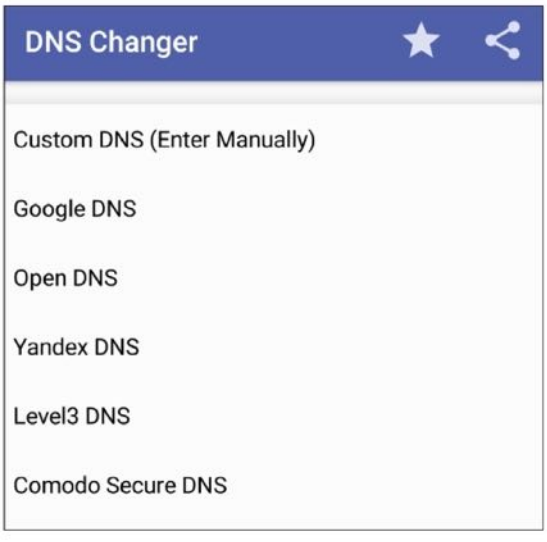
01 › ENTRER UN DNS MANUELLEMENT



DNS Changer propose un peu moins d'une dizaine de DNS, dont OpenDNS et Google Public DNS. Si vous ne trouvez pas votre bonheur dans la liste, touchez le nom du DNS actif et choisissez **Custom DNS (Enter Manually)**. Tapez l'adresse du **DNS 1** et du **DNS 2** (qui prend le relais en cas de problème). Nous vous conseillons ceux d'OpenNIC (**www.opennicproject.org**), respectueux de la vie privée.

02 › UTILISER LES DNS PRÉ-ENREGISTRÉS

La manipulation est la même qu'à l'étape précédente, sauf que vous choisissez ici un DNS de la liste. Dans les deux cas (manuel ou pré-enregistré), touchez le bouton de lecture pour valider le changement de DNS. Retouchez le bouton pour revenir au DNS par défaut de votre appareil Android.

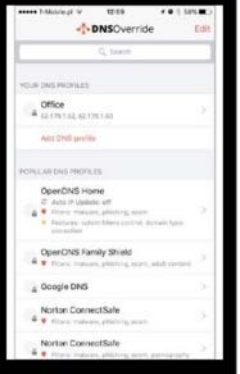


03 › RÉSOUDRE LES PROBLÈMES DE CONNEXION

Si vous êtes connecté au Wi-F-i, la première activation d'un nouveau DNS va le couper. Normalement, vous pouvez vous y reconnecter dans la foulée. Si cela ne fonctionne pas, attendez une minute avant de réessayer. En cas de problème prolongé, redémarrez l'appareil.

ET DU CÔTÉ DE LA POMME ?

Le principe est exactement le même que l'on roule pour la pomme ou le petit robot vert. Sur iPhone et iPad, essayez DNS Override, qui fonctionne aussi bien en Wi-Fi qu'en 3G/4G. L'appli intègre plus d'une dizaine de serveurs reconnus, dont OpenDNS, Google Public DNS et Norton ConnectSafe.



Lien : **https://goo.gl/Z4gJNC**

L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

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* ?

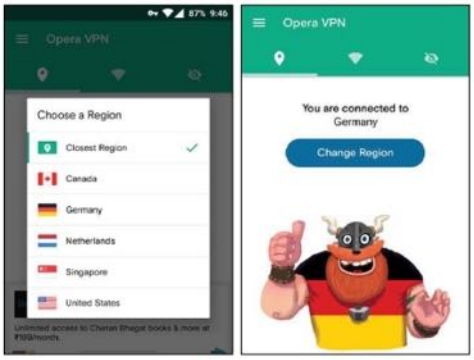
Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

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.

UN VPN SUR VOTRE IPHONE

// AVEC OPERA VPN

Opera vient de lancer un VPN à la fois gratuit et illimité sur iOS. Utilisés principalement pour chiffrer les communications entre votre mobile et un hotspot public pour éviter les fuites de données et les attaques de pirates, les VPN permettent aussi d'accéder aux contenus internationaux des Netflix, Hulu, etc. Le VPN d'Opera va même bloquer les publicités et les divers trackers qui viendraient tenter d'en savoir un peu trop sur vos habitudes de navigation.



https://goo.gl/v2jkEZ

PROTÉGER VOTRE VIE PRIVÉE

// AVEC CM BROWSER

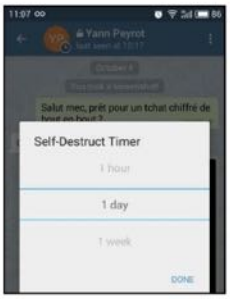
Sur Android, chaque navigateur a sa spécialité: la synchronisation pour Chrome, les extensions pour Firefox, la vitesse pour Dolphin... CM Browser a choisi la sécurité et la vie privée. Ouvrez le menu latéral en pressant le logo à trois carrés à côté de la barre d'URL ou en faisant glisser votre doigt de la droite vers la gauche, puis pressez **Passer en navigation privée**. Pour ne pas être suivi par les sites web que vous visitez, pressez le bouton menu de l'application (trois traits horizontaux). Touchez **Sécurité** et cochez **Ne pas suivre**. Cochez aussi **Prévention de la fraude** et **scan des Téléchargements**, votre navigation sera ainsi plus sécurisée. Vous n'êtes pas le seul à utiliser cet appareil, ou vous voulez effacer vos traces? Toujours dans les **Données personnelles**, cochez **Effacer l'historique en quittant** et décochez **Restaurer les onglets au démarrage** et **Se souvenir des mots de passe**.

https://goo.gl/XnYIdi

UTILISER LA FONCTION SECRET CHAT

// AVEC TELEGRAM

Le Secret Chat, c'est une discussion à deux très sécurisée, chiffrée de bout en bout, et dont vous pouvez programmer l'autodestruction. Dans Telegram, touchez le menu «hamburger» (les trois traits parallèles) puis **New Secret Chat**. Appuyez sur le contact que vous voulez y inviter. Le Secret Chat est une discussion à deux uniquement. Tout ce que vous faites sur le Secret Chat est communiqué à votre interlocuteur (les captures d'écran par exemple). Il est également impossible de transférer les messages du Secret Chat. Pour effacer le Secret Chat sur les deux appareils au bout d'un temps donné, appuyez sur les trois points verticaux puis **Set self-destruct timer**. Choisissez une durée et validez avec **Done**. Attention: seuls les messages écrits après la programmation seront supprimés.



https://telegram.org

DUPER LES MOUCHARDS

// AVEC GHOSTERY

Ghostery voit ce qui ne se voit pas sur Internet. Il détecte les mouchards, les balises placées sur les pages Web par les réseaux publicitaires et les scripts qui veulent enregistrer vos activités. L'appli contient un module qui va recueillir des données anonymes sur les mouchards pour avertir les autres utilisateurs de Ghostery. Cette extension peut empêcher que les éléments de page qu'il détecte s'exécutent dans votre navigateur. Vous pourrez ainsi contrôler la manière dont le suivi de vos données de navigation est effectué. Attention, car le fait de bloquer les mouchards peut avoir des conséquences inattendues sur les sites visités. Certains peuvent être utiles. À vous de faire le tri dans la liste.

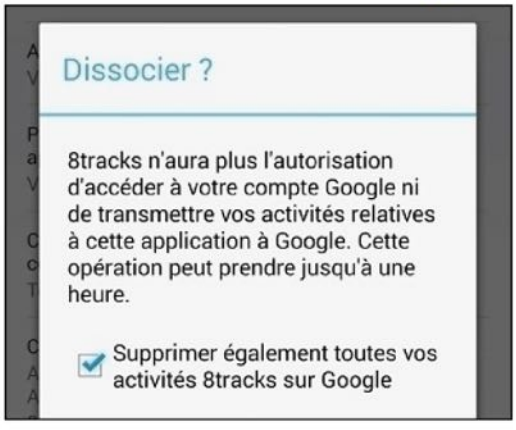
www.ghostery.com

EMPÊCHER LES APPLICATIONS D'ACCÉDER À GOOGLE+

// AVEC VOS PARAMÈTRES ANDROID

Certaines applis sont associées par défaut au réseau social made in Google. Cela leur donne la permission d'interagir avec votre compte. Allez dans **Google+**, connectez-vous, appuyez sur les trois points verticaux puis sur **Paramètres > Paramètres du compte**. Touchez votre adresse mail et **Apps avec Google+ Sign-In**. Sélectionnez une appli puis **Dissocier**, en cochant **Supprimer également toutes vos activités sur Google**, pour effacer les données transmises jusqu'à présent.

https://goo.gl/bS5DGT



CHOISIR CE QUE GOOGLE SAIT DE VOUS

// AVEC LES PARAMÈTRES GOOGLE

Vous ne pouvez pas empêcher le géant du Net d'obtenir des infos sur vous, mais les contrôler, oui. Tout en haut des **Paramètres Google**, ouvrez **Infos persos et confidentialité** et **Commandes relatives à l'activité**. C'est là que vous effacerez et désactiverez les différents historiques. Par exemple, **Activité sur le Web et les applications** concerne vos recherches et les pages visitées au travers des applis Google et du navigateur Web. **Activité vocale et audio** répertorie les recherches effectuées avec la commande «**OK Google**». **Historique des recherches YouTube** et **Historique des vidéos regardées sur YouTube** agissent sur l'enregistrement des données liées à vos visites sur le service vidéo.

UNE ALTERNATIVE À ORBOT

// AVEC FIRE.ONION

Si vous avez essayé notre solution d'anonymat Orbot/Orfox, mais que vous n'avez pas été convaincu, Fire.onion propose à peu près la même chose. Une fois connecté à Tor, le navigateur intégré vous propose de faire vos recherches sur le moteur DuckDuckGo. Bien sûr, l'appli est compatible avec les «hidden services» et leurs liens en .onion. Pour les possesseurs d'iPhone qui n'auraient pas été séduits par Onion Browser (voir page 59), il existe aussi Red Onion (**https://goo.gl/ZrpJSP**) que vous pouvez acheter pour 2 € sur l'App Store.

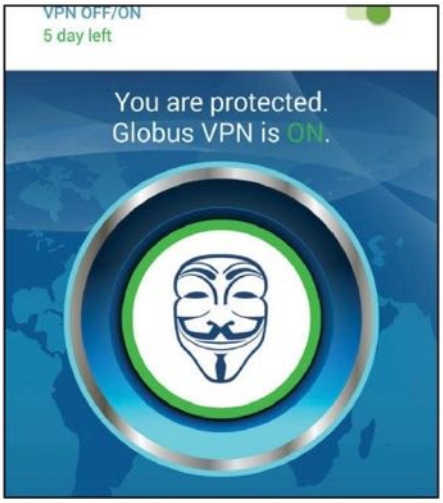
https://goo.gl/gwXZj0

UN COMBO GAGNANT POUR VOTRE ANONYMAT

// AVEC VPN GLOBUS PRO!

Encore un combo navigateur/Tor au programme ! VPN Globus Pro embarque une solution de VPN sûre fonctionnant de conserve avec Tor et un navigateur vierge de toute extension pour parfaire votre anonymat (ces dernières peuvent en effet vous «trahir» et révéler votre emplacement). L'appli est payante au bout de 5 jours, mais pour ce prix vous avez aussi la possibilité d'avoir un stockage chiffré en ligne.

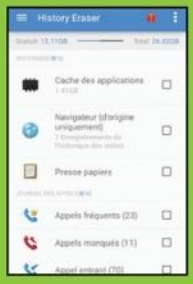
https://goo.gl/9jLbSd



SUPPRIMER L'HISTORIQUE DE NAVIGATION

// AVEC HISTORY ERASER

Pour faire le grand ménage sur votre smartphone sans pour autant installer une appli lourde, nous vous conseillons History Eraser. Il suffit de cocher les cases pour effacer en une seule fois, les vieux SMS, l'historique de navigation, les résidus d'anciennes applis, les métadonnées de conversations, etc.



https://goo.gl/q5DuWO

UN NAVIGATEUR QUI RESPECTE VOTRE VIE PRIVÉE

// AVEC DOLPHIN ZERO INCOGNITO BROWSER

Cette appli est un «fork» du très bon navigateur Dolphin sauf que cette version va automatiquement supprimer toutes les données sensibles lorsque vous allez la quitter: mots de passe stockés dans la mémoire vive, historique, cookies, métadonnées, formulaires, cache, etc. Dolphin Zero porte bien son nom puisqu'il ne comporte aucune option superflue permettant les vols de données: onglet, Flash et extensions. Malheureusement pour les possesseurs d'iPhone, il faudra débourser la somme de 3 € pour en profiter.

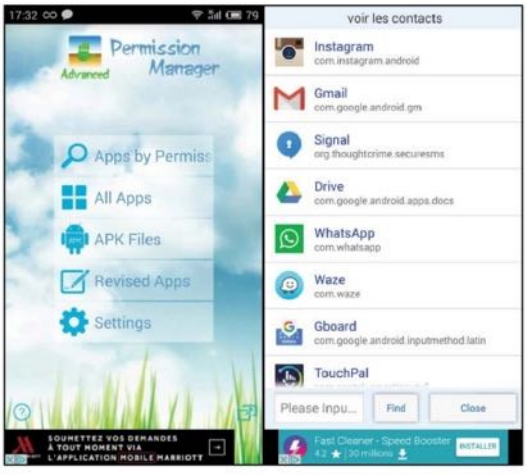
https://goo.gl/aH0lFx

GÉRER LES PERMISSIONS DES APPLICATIONS

// AVEC ADVANCED PERMISSION MANAGER

Vous êtes sous Android 6.0 Marshmallow ou sous 7.0 Nougat? La gestion des permissions des applis est une fonction native. Pour les autres, essayez Advanced Permission Manager. L'appli va créer une copie de celle dont vous aurez modifié les permissions. Il s'agit bien sûr de faire en sorte que certaines applications trop curieuses n'aillent fouiller dans vos contacts ou vos SMS par exemple. Attention: installer la nouvelle APK nécessite la désinstallation de l'originale. Sachez aussi que supprimer certaines permissions peut entraîner des dysfonctionnements. Le mieux est de faire des tests pour trouver ce que vous pouvez enlever ou non.

https://goo.gl/uy2yoF



BLOQUER DES NUMÉROS

// AVEC TRUECALLER

Vous souhaitez bloquer un contact ou éviter ces appels en numéro privé au beau milieu de la nuit? Truecaller va vous aider à retrouver la sérénité. Sélectionnez votre pays de résidence et saisissez votre numéro. Vous recevrez ensuite un appel du service Truecaller qui va vérifier que vous avez indiqué le bon. Inutile d'y répondre. Enfin, vous devrez créer un profil ou relier votre compte Truecaller à un réseau social.

Touchez l'icône à côté de **Truecaller**, en haut à gauche, et sélectionnez **Historique**. Choisissez le numéro ou le contact à bloquer et sélectionnez **Bloquer & Signaler**. Confirmez avec **Oui**. Le contact ne pourra plus vous appeler, ni vous envoyer de SMS. Faites apparaître le menu latéral, touchez **Bloquer** puis, dans le menu **Blocage**, sélectionnez **Numéros Inconnus**. Dans la nouvelle fenêtre, cochez **Appels** puis **Textos** et validez avec **OK**. Désormais, aucun numéro masqué ne pourra vous contacter.

www.truecaller.com

SURFER ANONYMEMENT

// AVEC DUCKDUCKGO

Vous n'êtes pas obligé de passer par Tor pour profiter du moteur de recherche DuckDuckGo. Certes, vous ne serez pas anonyme, mais vous éviterez que de grandes sociétés du Net ne volent vos données ou scrutent vos moindres recherches pour faire leur beurre.

https://duckduckgo.com/app

CHIFFREMENT

PROTÉGER VOS MOTS DE PASSE AVEC ENPASS

Les solutions pour mettre à l'abri vos sésames ne manquent pas. Enpass a l'avantage de ne demander aucune inscription et de stocker localement vos données tout en les chiffrant.

Toutes les infos que vous entreposez sur Enpass sont chiffrées à l'aide d'une clef AES 256 bits. Pour y accéder, une seule solution : renseigner le mot de passe maître. Le choix de ce dernier est important. Notre conseil sécurité : inventer une phrase de passe. Une suite de mots dignes du Kamoulox. Exemple : « Equateurpoulethierryscreenshot ». À la différence d'un service comme LastPass, Enpass ne vous expose pas à un piratage de vos données personnelles à distance. Les clefs de chiffrement sont en effet stockées localement et non sur un serveur distant.

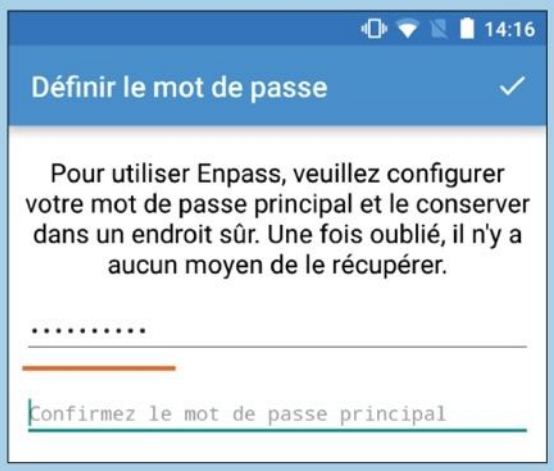
GRATUIT, MAIS PAS TROP...

Enpass sur mobiles est gratuit, mais vous propose un stockage limité jusqu'à 20 mots de passe. Pour passer outre cette limite, il faut vous acquitter de la coquette somme de 9,62 € sur Android et 9,99 € sur iOS. Ses concurrents proposent un système d'abonnement. Là, vous payez une seule fois et vous êtes tranquille... c'est à vous de voir.
Voici comment prendre en main l'appli sur Android. Ne vous inquiétez pas, les manipulations sont sensiblement les mêmes sur tous les OS.

ENREGISTRER SES MOTS DE PASSE

PRATIQUE

01 › CHOISIR LE MOT DE PASSE MAÎTRE



Le seul à retenir, car vous donnant l'accès à l'appli. Appuyez sur **Je suis un nouvel utilisateur d'Enpass**. Inventez ensuite votre sésame que vous renseignez dans le champ **Entrez le mot de passe principal**. Confirmez-le avant d'appuyer sur le ✓. Un indicateur (variant du rouge au vert) vous informe du niveau de sécurité de votre sésame principal.

02 › METTRE DE CÔTÉ UN MOT DE PASSE

Allez via le menu latéral dans **Identifiants**. Pressez le + puis nommez le service pour lequel vous souhaitez que l'appli retienne le mot de passe (dans notre exemple, il s'agit d'Amazon). Remplissez

les champs suivants: **Nom d'utilisateur**, **URL** et **Mot de passe**. Validez l'enregistrement du mot de passe en pressant ✓ **Terminé**.

03 › TROUVER UN MEILLEUR MOT DE PASSE

Sur la fiche d'un mot de passe, pressez le crayon pour activer les modifications. Appuyez ensuite sur le rouage à droite de **Mot de passe**. L'appli suggère un mot de passe sécurisé. Définissez une **Longueur** puis choisissez de le **Générer**. Rendez-vous ensuite sur le service dont vous venez de modifier le mot de passe afin d'enregistrer, via les paramètres du site, le nouveau.

UN COFFRE-FORT

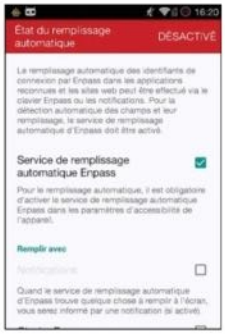
En plus de vos mots de passe, Enpass garde dans un coin des notes importantes. L'accès à ces dernières est protégé par un mot le mot de passe maître. Vous enregistrez également les infos liées à vos cartes bleues pour éviter d'avoir à les retaper lorsque vous achetez en ligne... stockez sereinement toutes ces données si sensibles sur Enpass pour les avoir partout avec vous.

UTILISER SES SÉSAMES

PRATIQUE

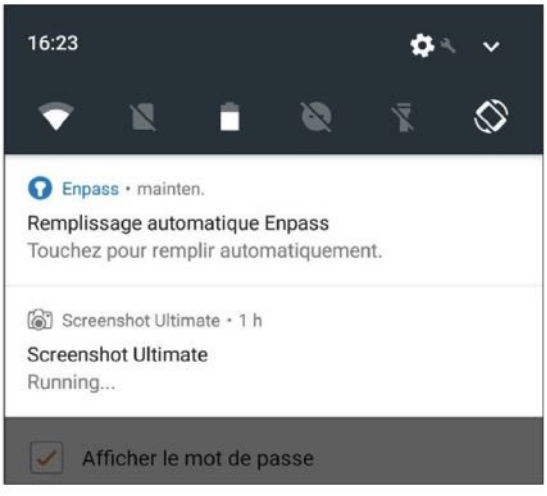
01 › RÉGLER ENPASS

Faites apparaître le panneau latéral pour choisir le rouage tout en haut à gauche. Ouvrez le menu **Remplissage automatique** puis cochez successivement **Service de remplissage automatique Enpass** et **Notifications**. Ainsi, vous profitez des services d'Enpass depuis n'importe quel navigateur Web.



02 › RENTRER AUTOMATIQUEMENT UN MOT DE PASSE

Rendez-vous sur le site dont vous venez de modifier le sésame. Au lieu de vous connecter de manière classique (en renseignant l'identifiant et le mot de passe associé), déroulez votre volet de notifications pour presser celle mentionnant **Touchez pour remplir automatiquement**. Appuyez ensuite sur l'icône du service souhaité pour y être automatiquement connecté.



03 › AJUSTER LE NIVEAU DE SÉCURITÉ

Enpass est quelque peu tatillon sur la sécurité. Pour corriger cela, ouvrez les **Paramètres** comme en étape 1 pour choisir **Sécurité**. Avec **Verrouiller après**, vous définissez le temps au bout duquel le mot de passe maître est à nouveau demandé. Décochez **Verrouillez en quittant** pour éviter d'avoir à taper votre mot de passe dès que vous basculez sur une autre appli.

UNE SOLUTION MULTIPLATEFORME

Android, iOS, BlackBerry ou encore Windows et Mac OS... Enpass est disponible sur quantité de systèmes d'exploitation. En l'installant sur tous vos appareils, vous partagez vos mots de passe entre ces derniers via le Cloud (Dropbox, Google Drive...).

INFOS [CRYPTOMATOR]
Où le trouver ? [**https://cryptomator.org**]
Difficulté :

CHIFFRER vos DONNÉES STOCKÉES SUR LE CLOUD

Pour plus de sécurité, chiffrez vos données depuis votre service de stockage en ligne préféré. Grâce à Cryptomator, vous réalisez l'opération depuis votre ordinateur ou votre smartphone.

Nous avons déjà abordé la solution Cryptomator dans le numéro 30 de Pirate Informatique. Ce logiciel gratuit crée un coffre-fort virtuel. Ce dernier se comporte comme un dossier rangé dans un coin de votre PC ou de votre mobile. Un mot de passe, défini par vos soins, en protège l'accès. Une fois renseigné, vous accédez à vos fichiers. Libre à vous d'en ajouter ou d'en supprimer. Notez que Cryptomator doit être installé sur toutes les machines depuis lesquelles vous souhaitez accéder à vos fichiers protégés.

STOCKER DANS UN CLOUD N'EST PAS UNE SOLUTION MIRACLE...À MOINS QUE CE SOIT CHIFFRÉ !

LA PROTECTION FACILE

Pour utiliser l'appli depuis votre smartphone, la déclinaison mobile de votre service de Cloud préféré doit y être installée (Google Drive, Dropbox, iCloud Drive...). C'est sur l'un d'entre eux que Cryptomator va créer le coffre-fort virtuel. Une fois le mot de passe défini et le coffre-fort verrouillé, vous êtes le seul garant de l'accès à ce dernier... n'égarez pas le précieux sésame ou vous ne remettrez jamais la main sur vos fichiers. Le chiffrement de vos données s'effectue en un instant. Vos fichiers se retrouvent sur le Cloud. Illisibles tant que vous ne déverrouillez pas l'accès à votre coffre-fort.

Nous vous montrons plus bas comment utiliser Cryptomator sur Android. L'interface est sensiblement la même sur iPhone. Vous vous y retrouverez facilement.

CRYPTER SES FICHIERS

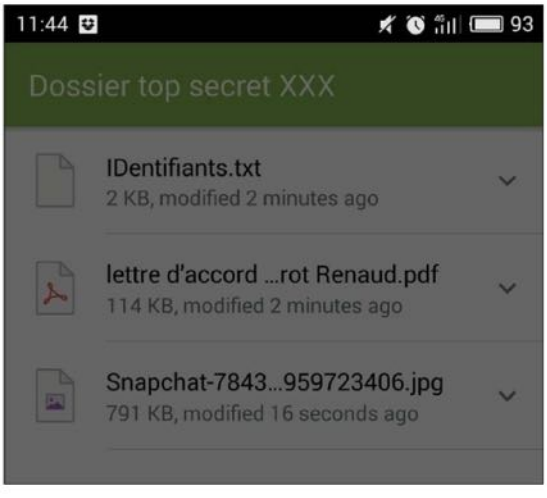
PRATIQUE

01 › CRÉER SON COFFRE

Installez Cryptomator depuis le lien mentionné plus haut. Pressez le + puis **Create New vault**. Sélectionnez votre service de Cloud (celui où sera placé votre dossier protégé). Nous utilisons ici Dropbox. Nommez votre coffre-fort puis appuyez sur **CREATE**. Définissez la localisation de votre coffre-fort avec **SET LOCATION** avant d'en choisir le mot de passe. Gardez-le précieusement.

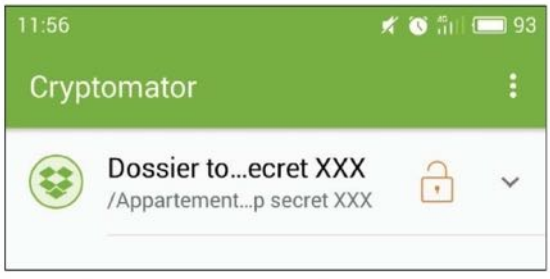
02 › STOCKER DES FICHIERS

Votre coffre-fort est verrouillé. Touchez ce dernier depuis la page principale de l'appli puis tapez le mot de passe. Pour ajouter des fichiers à votre espace, appuyez sur le + et **Upload Files**. Choisissez l'emplacement du fichier à téléverser. Cryptomator crée alors une copie du fichier pour le placer dans l'emplacement sécurisé. Avec **Create New folder**, vous créez un nouveau dossier.



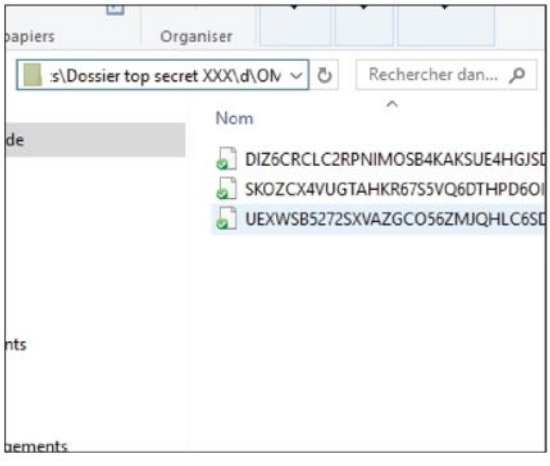
03 › SÉCURISER LE COFFRE

Une fois tous vos fichiers ajoutés dans le dossier crée via Cryptomator, retournez sur la page principale de l'application. Appuyez sur l'icône du cadenas. Ce dernier disparaît, signe que votre dossier est maintenant verrouillé. Pour retrouver l'accès, pressez à nouveau le dossier puis tapez le mot de passe.



04 › VÉRIFIER LE CRYPTAGE

Depuis votre ordinateur, ouvrez votre dossier Dropbox puis tentez d'explorer le contenu de celui crée via Cryptomator. Le dossier est bien là, mais tout ce qui se trouve à l'intérieur est illisible. Tant que vous n'installez pas Cryptomator sur cette machine et que vous ne déverrouillez pas le dossier via le mot de passe, vos fichiers sont à l'abri.



CHIFFRER VOTRE SMARTPHONE ANDROID

Comptes, paramètres, fichiers et applications : il est possible de chiffrer tout ce que contient votre téléphone. Pratique en cas de vol ou si vous avez des données sensibles, le chiffrement est accessible à tous, mais n'est peut-être pas une solution miracle pour tout le monde. Voyons de plus près les mécanismes d'Android...

Avant de se mettre à l'ouvrage, prenons quelques instants pour réfléchir. Avez-vous vraiment besoin de chiffrer le contenu de votre téléphone ? Si votre appareil est protégé avec un code ou un schéma de verrouillage, c'est peut-être suffisant pour mettre à l'abri vos photos ou autres documents stockés en local, votre compte Gmail ou Paypal. En cas de vol, le premier réflexe du malandrin sera d'effacer le contenu, de changer l'IMEI pour revendre votre Xpersung le plus vite possible sans aller chercher des photos de vos fesses dans les entrailles de la bête (ce qui est possible sans chiffrement, mais pas à la portée de tous).

LE CHIFFREMENT, INDISPENSABLE ?

Par contre, le chiffrement peut-être utile si vous avez des documents sensibles ou si vous êtes une cible potentielle pour l'espionnage ou que d'autres personnes que vous sont concernées par les données contenues sur votre téléphone : ingénieur, haut fonctionnaire, élu, journaliste, etc. Il faut aussi savoir qu'une fois le chiffrement activé, vous ne pouvez plus faire machine arrière à moins de réinitialiser votre appareil avec ses valeurs d'usine. Il faudra donc absolument faire une sauvegarde avant le chiffrement (car des accidents peuvent arriver) et avant un éventuel retour à la normale (vous avez changé d'avis, vous voulez vendre votre téléphone, etc.) Notez aussi que dans certains cas vous ne pourrez plus mettre à jour le système ou certaines applis de sécurité et que le chiffrement est parfois lourd pour les appareils les plus anciens ou d'entrée de gamme.

UN CHIFFREMENT QUI S'AMÉLIORE

Nous ne parlerons ici que du système Android puisque sur l'iPhone, depuis iOS8, le FDE (Full Encryption Disk) est devenu obligatoire. Sur Android, le FDE a été rendu disponible dès les versions 3 (Honeycomb pour tablettes) et 4 (Ice Cream Sandwich) mais il était malheureusement vulnérable aux attaques «off-device». Il est donc possible de brancher un téléphone sur un PC et de bidouiller le contenu avec ADB (Android Debug Bridge) pour retrouver le contenu chiffré. Il faudra bien sûr lancer une attaque « brute force » peu évidente, mais le risque est bien là. L'arrivée de la version Lollipop 5.0 a changé la donne. Non seulement le chiffrement est proposé lors du premier lancement, mais les mécanismes de chiffrement ont évolué. Dorénavant, une clé 128 bits est générée au premier lancement, elle est ensuite hashée (SHA256) et signée dans une partie hardware du téléphone et pas simplement dans la mémoire flash. Les risques de fuite sont donc à ce jour nuls. Google a même senti le vent du changement puisque sur ses Nexus, le chiffrement est obligatoire sur le système 5.0. La bonne nouvelle, c'est que de la version 3 à la version 7 (Nougat), le processus de chiffrement est le même pour l'utilisateur.

L'INDUSTRIE S'INTÉRESSE DE PLUS EN PLUS AU CHIFFREMENT CAR LES UTILISATEURS S'Y INTÉRESSENT !

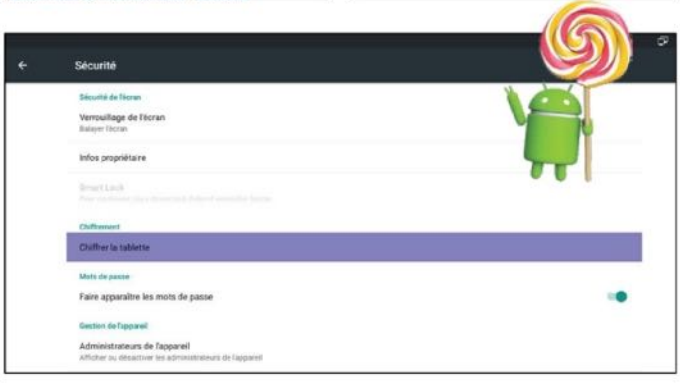
BRUTE FORCE ?

La "force brute" est une méthode de récupération de mot de passe qui consiste à essayer toutes les combinaisons de caractères pour tomber sur la bonne entrée. Le logiciel va essayer toutes les combinaisons de lettres, de chiffres et autres caractères pour arriver à ses fins. Pour un voleur, l'attaque «brute force» est difficile à mener puisque le système le fera patienter durant de longues secondes toutes les 10 tentatives infructueuses. Avec des techniques poussées, cela est pourtant possible d'où l'intérêt de bien choisir son mot de passe et de faire des mises à jour du système pour colmater les failles dé sécurité.

CHIFFRER LE CONTENU DE VOTRE SMARTPHONE ANDROID

01› LES OPTIONS DE SÉCURITÉ

Rappelons avant de commencer qu'il faudra faire une sauvegarde de vos données avant de chiffrer votre téléphone. Allez dans **Paramètres** puis sélectionnez **Sécurité**. Suivant la marque de votre appareil et votre version d'Android, vous trouverez l'option **Chiffrer l'appareil** ou **Crypter le téléphone**.

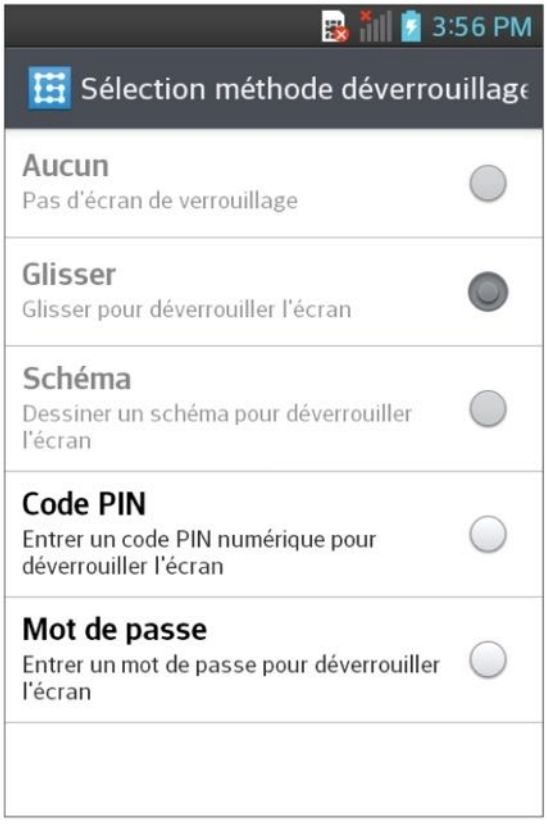


02› PRENEZ VOS PRÉCAUTIONS

Il faudra ensuite suivre les instructions. La plupart du temps, on vous demandera de brancher le téléphone sur secteur ou de démarrer le processus avec 80% de batterie disponible. Car en interrompant le processus, vous perdrez vos données.

03 › LE MODE DE VERROUILLAGE

Sélectionnez ensuite un mode de déverrouillage. Encore une fois, selon la marque et la version du système, les options peuvent varier. Si vous utilisez une version antérieure à Lollipop (5.0), utilisez un mot de passe solide à la place d'un PIN standard pour rendre difficile l'attaque «brute force».



04 › LAISSEZ LE CHARME AGIR!

Après avoir saisi votre sésame, vous devrez une nouvelle fois valider pour commencer le processus de chiffrement. Le délai est variable suivant la quantité de données que vous avez stockées, mais il ne devrait pas dépasser une heure. Votre téléphone devrait redémarrer plusieurs fois, alors surtout ne faites pas de manipulation hasardeuse!

GÉNÉRER DES MOTS DE PASSE EFFICACES

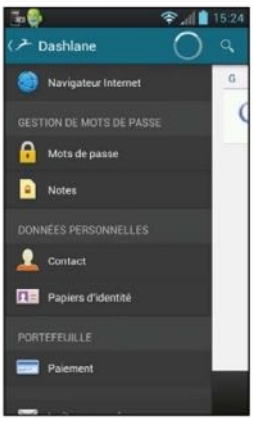
// AVEC PASSWORD GENERATOR

123456, motdepasse, password, jaipasdidées... si le choix de mots de passe de ce type reste très drôle, du côté de l'aspect sécurité, ce n'est pas ce qu'il y a de mieux. Password Generator le fait pour vous. Sélectionnez le nombre de caractères dont vous avez besoin et le tour est joué. L'appli choisit chaque lettre de manière complètement aléatoire, ce qui renforce considérablement la «force» du précieux sésame puisqu'il n'a aucune signification... la seule limite, c'est votre mémoire. Pour iOS, il faudra utiliser Free Password Generator (**https://goo.gl/2RfqWw**). L'appli est gratuite et ne nécessite pas de jailbreak.

https://goo.gl/0gB3Rn

DES MOTS DE PASSE BIEN PROTÉGÉS

// AVEC DASHLANE



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. L'appli va encore plus loin puisqu'elle 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. Attention, 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. Passé ce délai, il faudra payer 40€/an.

www.dashlane.com

DU CHIFFREMENT NATIF SUR LES COMMUNICATIONS

// AVEC OVERSEC

Vous le savez bien, lorsqu'il s'agit de chiffrer des communications, il faut que les correspondants utilisent le même logiciel/protocole pour que cela fonctionne. Cela peut décourager le plus motivé des utilisateurs puisqu'il faudra «convertir» vos amis et contacts à telle ou telle solution de chiffrement. Sur Android, la solution pourrait s'appeler Oversec : une application qui ajoute une couche de chiffrement de bout en bout à toutes les autres applications. A vous les SMS, Facebook, Twitter, Skype, ou Gmail entièrement chiffrés ! Oversec n'est donc pas restrictif et s'applique potentiellement à chacune de vos applications. Il est même possible d'afficher de faux textes qui s'afficheront en clair sur le réseau pour détourner l'attention des espions/pirates.

www.oversec.io

MASQUER SES PHOTOS ET VIDÉOS

// avec Hide It Pro

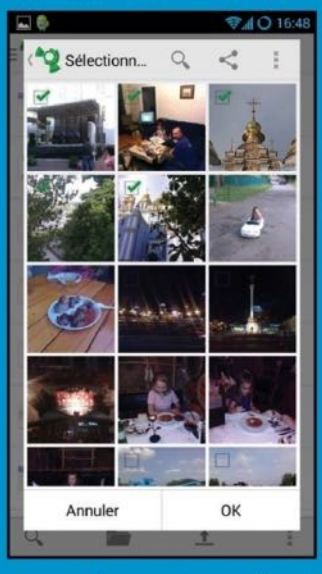
Hide It Pro prend le nom d'Audio Manager sur votre téléphone, pour plus de discrétion. Restez appuyé sur le logo du haut pour accéder à l'interface. Vous devrez aussi définir un code PIN. Choisissez ensuite les éléments à camoufler à l'aide des différentes rubriques (**Pictures** pour les photos, **Videos**, **Music**...) ou de l'explorateur de fichiers (**File Manager**). Une fois vos choix effectués, touchez **Hide Selected Files** pour commencer à cacher les fichiers compromettants. Ces derniers deviendront uniquement accessibles depuis l'application Hide it Pro.

https://goo.gl/eib8Al

UN COFFRE-FORT SUR VOTRE MOBILE

// avec BoxCryptor

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 (OneDrive, Google Drive, DropBox, etc.) 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.



www.boxcryptor.com

CHIFFRER VOS DOCUMENTS

// avec Secrecy

Si vous avez une vieille version d'Android ne prenant pas en charge le chiffrement natif des fichiers, vous pouvez utiliser Secrecy. L'appli 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 toutes les applications. Si vous désinstallez Secrecy ou que vous exportez vos conteneurs chiffrés vers un PC par exemple vous pourrez les déchiffrer avec un logiciel compatible AES 256 comme 7Zip. Sur iPhone il existe l'application Best Secret Folder (**http://goo.gl/jYQl3E**) qui permet de cacher photos et vidéos dans un dossier spécial protégé par un mot de passe. Pas de chiffrement au programme à moins de chercher dans Cydia.

http://goo.gl/0NOsSE

MULTIMÉDIA

STREAMER DES TORRENTS SUR MOBILE

Vous n'arrivez pas à choisir entre le stream et le BitTorrent ? Vous ne voulez pas sacrifier l'immédiateté du premier pour la qualité du second ? Aucun problème : Popcorn Time permet de voir directement un film à partir de BitTorrent. Le meilleur des deux mondes.

C'est bien pratique ces smartphones et tablettes pour regarder des vidéos dans son lit ou sur son canapé, sans monopoliser un écran. Problème : vous aimeriez bien regarder ce Blu-ray acheté plus tôt, et vous avez beau le retourner dans tous les sens, votre appareil n'a pas de lecteur de disque. Copier le film depuis le PC et le transférer ? Fastidieux, et puis vous n'avez pas assez d'espace de stockage. Reste la solution du streaming. Dans ce domaine, difficile de trouver mieux que Popcorn Time, ce service mélangeant téléchargements et torrents. Disponible pour Android et iPhone, le choix est énorme : films, séries TV, animes... Du moment que vous restez centré sur l'Occident (à part les animes, il y a très peu de films asiatiques, même cultes), vous trouverez votre bonheur.

COMMENT ÇA MARCHE ?

Pas de client, de téléchargement ou de ratio à gérer ici. Choisissez votre film, sa qualité d'image et les sous-titres (options pas toujours disponibles) et c'est parti ! Vous pouvez même avancer pour passer un générique sans tout faire planter. En revanche, pour ce genre d'utilisation, le fichier doit être en « bonne santé » et donc posséder suffisamment de « seeders » pour que la vidéo ne saccade pas. Nous vous rappelons que Popcorn Time doit être utilisé uniquement pour streamer les films et séries dont vous possédez une copie légale.

POPCORN TIME PROFITE D'UNE INTERFACE INTUITIVE ET D'UN CATALOGUE ÉTOFFÉ POUR ANDROID ET IOS

INFOS [POPCORN TIME]

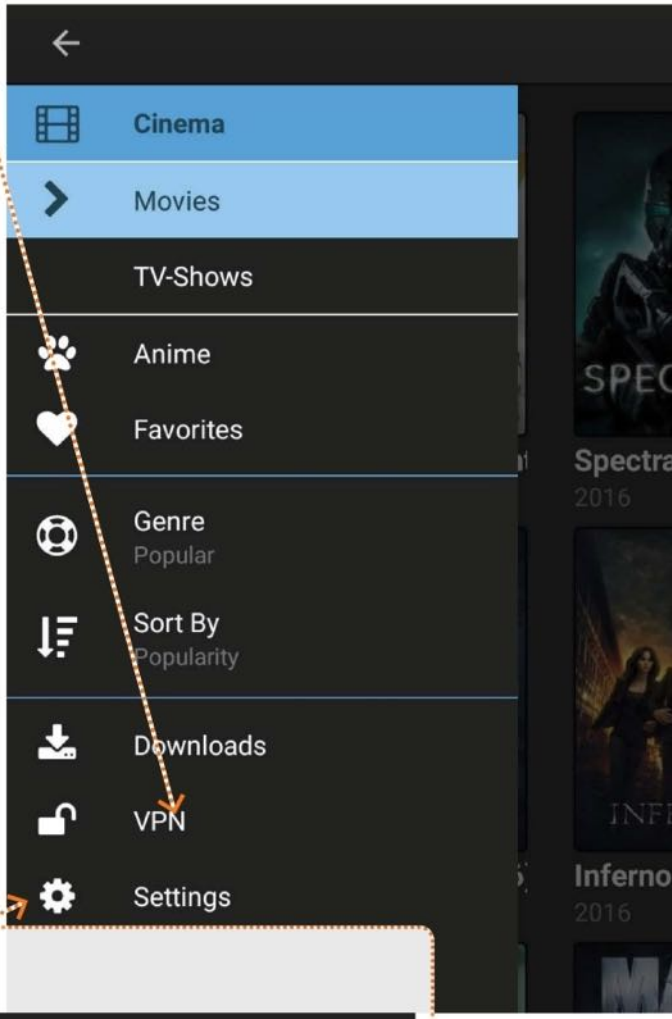
Où le trouver ? [Android > **https://goo.gl/BPw01J**] [iOS > **https://goo.gl/7s07Py**]

Difficulté :

L'INTERFACE DE

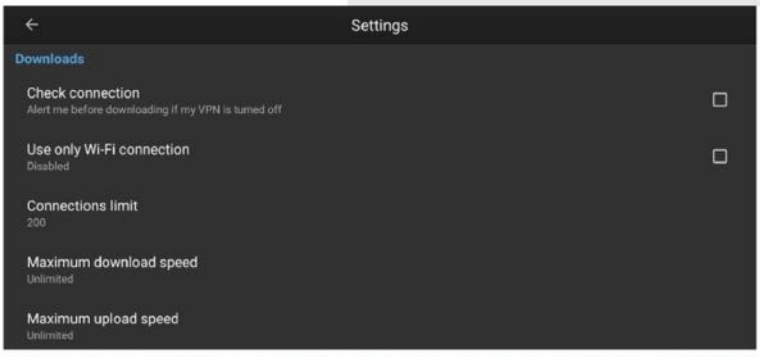
LE VPN

Il fut un temps où Popcorn Time proposait un VPN intégré (pour chiffrer votre connexion Internet et vous rendre anonyme). Aujourd'hui, l'option renvoie à la souscription d'un abonnement payant. Mais comme vous utilisez l'application pour streamer les DVD et Blu-ray que vous avez achetés, vous n'en avez pas besoin

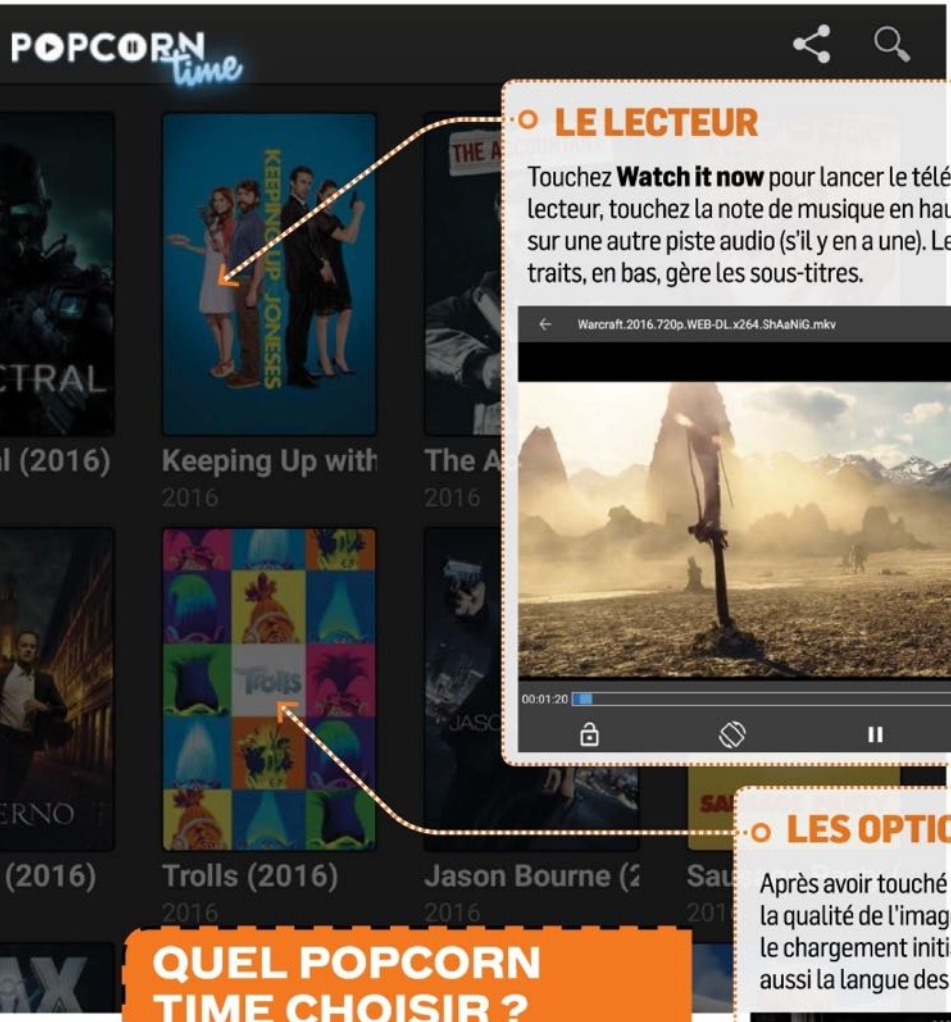


LES PARAMÈTRES

Descendez jusqu'à **Download** pour contrôler la vitesse de connexion. Nous vous conseillons **Unlimited** pour les deux options (**download** et **upload**).



POPCORN TIME

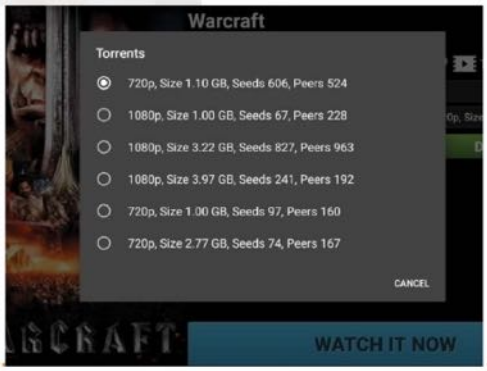


LE LECTEUR

Touchez **Watch it now** pour lancer le téléchargement initial. Sur le lecteur, touchez la note de musique en haut à droite pour basculer sur une autre piste audio (s'il y en a une). Le rectangle blanc avec des traits, en bas, gère les sous-titres.

LES OPTIONS DU FICHIER

Après avoir touché un film, vous pouvez choisir la qualité de l'image. Plus il y a de Seeds, plus le chargement initial sera rapide. Choisissez aussi la langue des sous-titres le cas échéant.



QUEL POPCORN TIME CHOISIR ?

Une recherche sur Popcorn Time dans Google ou autre donne popcorntime.to, mais aussi .sh ou encore .io. Les sites sont d'ailleurs identiques, à l'exception des numéros de version de leurs logiciels et applications. Dans les faits, il n'y a quasiment aucune différence entre ces branches du Popcorn Time original. Nous avons choisi le .to qui nous semble plus actif sur les mises à jour de son appli.

REGARDER LA TÉLÉ EN DIRECT OU EN REPLAY

Au lieu de jongler entre plusieurs applications de chaînes de TV, optez pour Molotov. Elle regroupe direct et replay pour toute la TNT. Sur Android ou iPhone/iPad.

Regarder la télévision sur une télévision ? C'est so 2000 ! La TV, on la regarde sur son mobile ou sa tablette, en direct ou en replay. Le principe n'est pas nouveau, et plusieurs groupes ont depuis longtemps lancé leur application dédiée : 6play, MyTF1, francetv pluzz... Le problème, c'est que pour profiter de tous les programmes de la TNT, il faut jongler entre ces différentes applis. Mais ça, c'était avant Molotov TV.

UNE APPLI POUR LES REGROUPER TOUTES

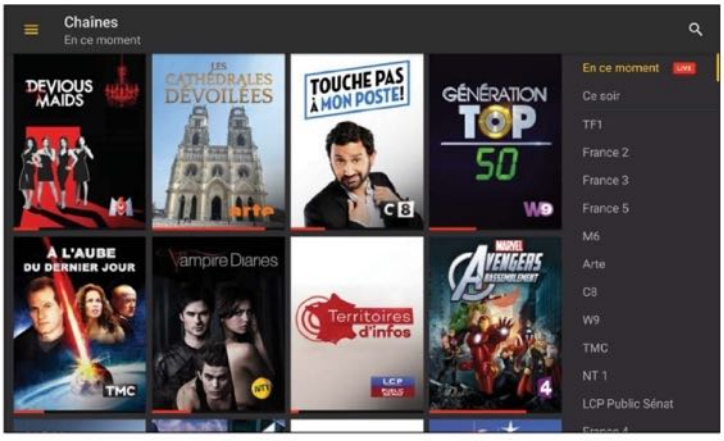
Molotov TV, c'est 36 chaînes accessibles gratuitement. Toutes celles de la TNT, auxquelles s'ajoutent NoLife ou EuroNews par exemple. L'interface de l'application se prend en main en quelques secondes. Vous pouvez reprendre le direct là où vous en étiez, mettre des programmes ou des personnalités en favori pour être prévenu de leur passage dans une série ou autre... Bref, profiter de la télévision comme vous en avez envie. Les plus accrocs d'entre vous pourront passer à plus de 70 chaînes, moyennant 10 € par mois.

LES ALTERNATIVES ?

L'avantage de Molotov, c'est que son utilisation est gratuite et indépendante de votre abonnement Internet. Mais pour les chaînes de votre bouquet TV, il n'y a pas 36 solutions : utilisez l'application officielle de votre fournisseur d'accès (SFR TV, B.tv, TV d'Orange...). Les amateurs de programmes anglo-saxons peuvent aussi jeter un œil à MobiTV.

PROFITER DE LA TV SUR MOLOTOV

PRATIQUE

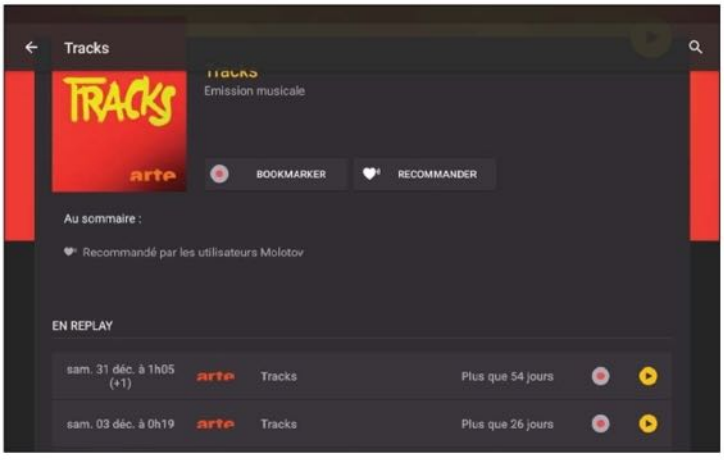


01 › PARCOURIR L'INTERFACE

Pour utiliser Molotov, vous devez créer un compte. Deux possibilités : utilisez Facebook ou une adresse mail classique. Faites votre choix, sachant que vous devez toucher le lien de validation pour activer votre compte. Via **En ce moment**, vous lancez le direct des chaînes mentionnées.

02 › EXPLORER LES PROGRAMMES

Faites glisser votre doigt de la gauche vers la droite pour afficher le panneau latéral. Depuis ce dernier, vous faites le tri entre les émissions (**Divertissement**, **Sport**, **Séries**...). Via **Parce que vous suivez...**, vous ajoutez des personnalités (avec **Suivre**) pour être tenu au courant des programmes les incluant.



03 › PROFITER DU REPLAY

Si vous avez manqué une émission et que vous savez que cette dernière est diffusée en replay, recherchez-la via la loupe en haut à droite. Lancez ensuite le replay de la date souhaitée en touchant le bouton lecture accolé. Via **Bookmarker**, vous placez le programme en favori. Pour ne pas passer à côté des futurs épisodes.

INFOS [ACESTREAM]

Où le trouver ? [**https://goo.gl/SHVse0**]

Difficulté :

SPORT LIVE : OL'ALLIANCE DU STREAM ET DU P2P

Ace Stream est un logiciel russe permettant de streamer à la fois des films et des séries en utilisant de banals fichiers Torrents, mais il concurrence aussi le stream traditionnel en ce qui concerne les retransmissions sportives en direct...

Pourquoi se contenter d'une retransmission sportive en stream toute moche et saccadée quand on peut appeler la technologie P2P à la rescousse. Disponible sous Windows, AceStream est aussi disponible sous Android où il propose la même chose : voir des matchs en direct en utilisant des liens spécifiques dérivés du Torrent. Ce logiciel concurrence en fait le logiciel SopCast ! En effet, le logiciel chinois partage maintenant la vedette avec le nouveau venu russe. Il suffit de regarder le nombre de liens distillés sur les sites spécialisés pour se rendre compte que Ace Stream est devenue la nouvelle référence pour le sport en direct. Vous trouverez des liens facilement sur le Net mais la référence s'appelle toujours **http://livetv.sx/frx**, un site russe lui aussi...

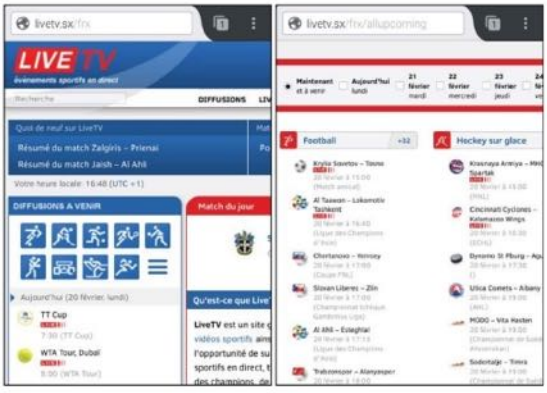
SOPCAST DÉCLINE MAIS ACE STREAM PREND LA RELÈVE !

ACESTREAM SUR ANDROID

PRATIQUE

01 L'INSTALLATION

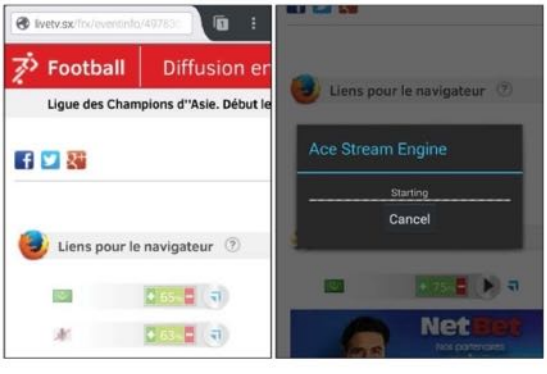
Téléchargez AceStream et profitez-en pour installer un lecteur multimédia comme MX



Player par exemple. En effet, l'appli n'en dispose pas. Vous n'avez besoin de faire aucun réglage. Allez sur le site LiveTV (voir plus haut) et trouvez votre match (foot, rugby, hockey, F1, hand, etc.) et affichez les liens.

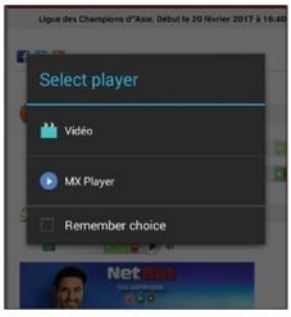
02 LES LIENS

Dans la liste vous trouverez des liens stream aec plein de pubs, des liens SopCast (un autre logiciel de retransmission TV) et des liens AceStream. Suivant la popularité du Live, vous aurez bien sûr plus ou moins de choix. Cliquez sur la petite icône bleue et pas sur la flèche noire sur fond gris.



03 LE CHOIX

AceStream va démarrer et vous demander de choisir un player vidéo. Au bout de quelques dizaines de secondes, la vidéo va charger. Vous n'aurez presque aucune pub et la qualité de la vidéo vous surprendra. Si vous avez des saccades, essayez un autre lien ou tentez de trouver un Live dans votre langue (les drapeaux de Live TV sont parfois trompeurs).



ET DU CÔTÉ DE LA POMME ?

Si vous n'avez pas d'appareil jailbreaké, vous pouvez lire les vidéos de stream «standard» du site Live TV avec le navigateur payant Skyfire. Pas top. Pour les heureux possesseurs de Cydia, il existe la possibilité de paramétrer des plugins «sportifs» dans Kodi (ex-XBMC) pour ensuite profiter des liens AceStream et Sopcast .. Ouf !

INFOS [µTORRENT (PC OU MAC)] Où le trouver ? [**https://goo.gl/SHVse0**]
[µTorrent Remote] Où le trouver ? [**https://goo.gl/Qjp30o**]
Difficulté :

GÉREZ VOS TORRENTS À DISTANCE !

Il n'est pas évident de télécharger des Torrents lorsqu'on travaille ou que l'on est rarement à la maison. Pour amorcer, surveiller ou gérer ses téléchargements à distance, il existe cependant des solutions toutes simples sur mobiles. Suivez le guide...

Pour optimiser au mieux ses téléchargements, on était autrefois obligé de sauvegarder ses Torrents sur une clé USB pour les rapporter chez soi le soir et enfin commencer le rapatriement des fichiers. Rares sont en effet les jobs ou les bibliothèques universitaires où l'on peut télécharger sans être inquiété.

UNE SOLUTION POUR CHAQUE CAS DE FIGURE

Pour avoir ses fichiers prêts à l'emploi à l'heure de l'apéro ou tout simplement gérer ses téléchargements lorsque vous n'êtes pas à la maison, la société BitTorrent a pensé à tout ! L'astuce consiste à paramétrer son client BitTorrent pour autoriser son contrôle à distance. Des logiciels comme µTorrent ou le client historique BitTorrent (qui propose la même interface) permettent ce genre de passe-passe. Vous pourrez accéder à votre client Torrent depuis une interface Web mais aussi sur mobiles : Android ou iOS !

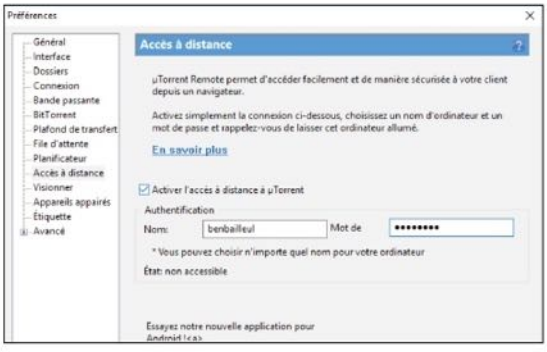
PAS BESOIN D'ÊTRE CHEZ VOUS POUR CONTRÔLER VOS TÉLÉCHARGEMENTS...

µTORRENT VIA L'APPLI MOBILE

PRATIQUE

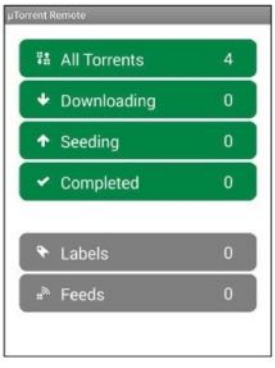
01 › SUR VOTRE PC/MAC

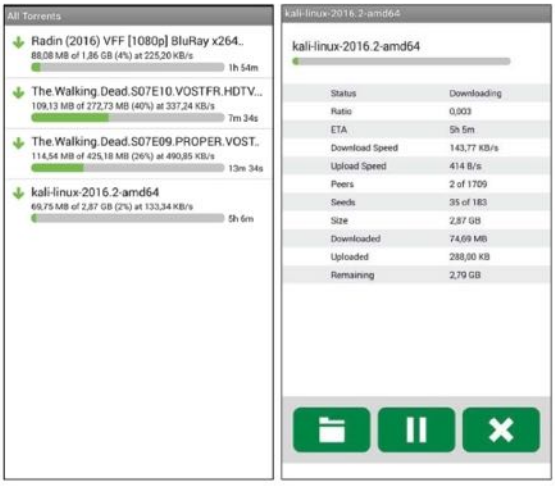
Commencez par télécharger la dernière version de µTorrent et installez-la. Dans **Options**> **Préférences**, sélectionnez **Accès à distance** dans le menu de gauche et cochez la case **Activer l'accès à distance µTorrent**. Définissez un mot de passe, un identifiant puis paramétrez une question de sécurité au cas où vous perdriez ces informations. Au bout d'un moment, le logiciel va vous avertir que l'inscription est terminée.



02 › SUR VOTRE MOBILE

Depuis votre mobile ou un PC distant, vous pouvez vous connecter au site **https://remote.utorrent.com** mais vous pouvez aussi utiliser l'appli mobile µTorrent Remote. Entrez les identifiants que vous avez choisis dans votre client sur votre PC/Mac et vous pourrez voir l'avancée des téléchargements, mettre en pause ou voir le détail des fichiers.

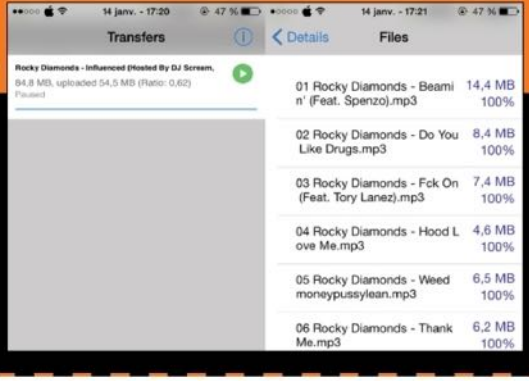




ET DU CÔTÉ DE LA POMME ?

Les possesseurs d'iPhone peuvent avoir la même appli de contrôle µTorrent que sur Android à condition d'être sous iOS 8 (suivre notre lien plus bas). Pour les autres, il faudra se contenter de l'interface WebUI à afficher dans le navigateur à cette adresse : **https://remote.utorrent.com**

Lien : **https://goo.gl/wiln2z**



DES SOUS-TITRES FACILES

// AVEC VLC MEDIA PLAYER

Le lecteur multimédia VLC reste le plus complet et le plus facile à appréhender. Depuis ce dernier, vous regardez confortablement films, séries, documentaires, etc. Lancez l'appli, cette dernière détecte automatiquement les fichiers vidéo stockés sur votre tablette ou smartphone. Touchez-en un depuis **Vidéo** pour le lire. Pressez à nouveau l'écran pour contrôler la lecture. Pour obtenir les sous-titres en français du film ou de la vidéo que vous regardez, pressez l'écran pour choisir l'icône ressemblant à une bulle de conversation. Là, touchez **Télécharger des sous-titres**. Vous activez ces derniers avec **Sous-titres**, au-dessus.

www.videolan.org/vlc

YOUTUBE SANS ALLUMER L'ÉCRAN

// AVEC NONSTOP YT

À cause de la publicité, YouTube ne permet pas de fonctionner sans écran. SI vous voulez utiliser cette plate-forme comme d'un walkman (comment ça, c'est quoi un walkman?), c'est fichu à moins de se promener avec une centrale nucléaire sur soi. NonStop YT se télécharge en fichier .apk en suivant notre lien. L'utilitaire évite l'interruption de la vidéo en cours de lecture quand vous mettez en veille votre mobile. Utilisez la loupe pour rechercher une vidéo en particulier et explorez les différentes catégories en faisant défiler la page vers le bas. Pour débuter la lecture d'une vidéo, appuyez sur la miniature de celle-ci. Grâce à l'appli, même en mettant votre mobile en veille (via Power), le son de la vidéo continue à être diffusé. Sous iOS, il faudra utiliser Mikoto (qui permet l'utilisation de YouTube en background) depuis le dépôt Karen's Pineapple sur Cydia.

https://goo.gl/8GtTOV

ENVOYER DES FICHIERS MULTIMÉDIAS LOURDS

// AVEC WETRANSFER

Vous cherchez à faire parvenir votre vidéo de vacances à l'un de vos proches ? Installez **WeTransfer**. L'appli scanne la mémoire interne de votre tablette. Présélectionnez ensuite les fichiers puis touchez **Next**. Renseignez l'adresse mail de votre destinataire dans le champ **to** puis écrivez un **message** avant de choisir **transfer**. Votre correspondant reçoit un lien direct pour télécharger le fichier.

https://wetransfer.com/apps

ENREGISTRER VOTRE ÉCRAN

// AVEC AZ SCREEN RECORDER

Pour capter le flux vidéo de votre écran, utilisez AZ Screen Recorder. Lancez l'appli puis touchez, via le menu qui apparaît sur votre gauche, l'icône représentant une caméra. Vous mettez fin à l'enregistrement via la commande stop, accessible depuis votre volet de notifications. Pour enregistrer une de vos sessions de jeu, Skype, un snap un peu trop rapide...

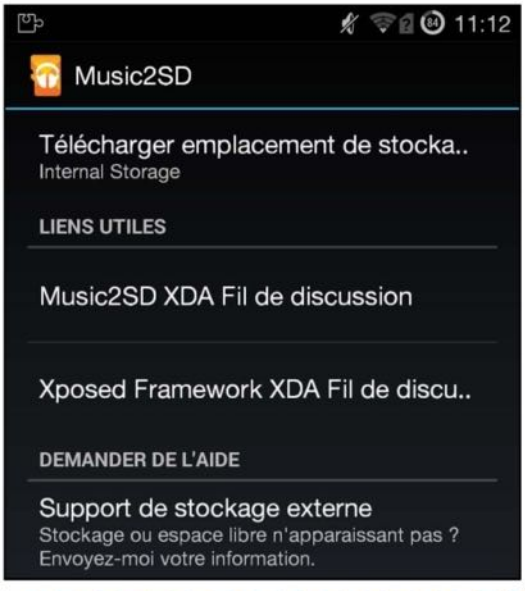
https://goo.gl/naSxEw

MIGRER LES MORCEAUX DE GOOGLE PLAY MUSIQUE

// AVEC MUSIC2SD

Google Play Musique refuse de vous laisser mettre vos morceaux sur la carte SD. Problématique lorsque la mémoire interne est pleine ou limitée... Heureusement, **Music2SD** force la création d'un emplacement sur la carte pour y stocker vos MP3. Installez le framework Xposed, puis Music2SD. Ouvrez ensuite le module Music2SD dans Xposed et redémarrez votre téléphone.

https://goo.gl/U93DSC



TRICHER AUX JEUX VIDÉO

// AVEC GMD SPEED TIME LITE

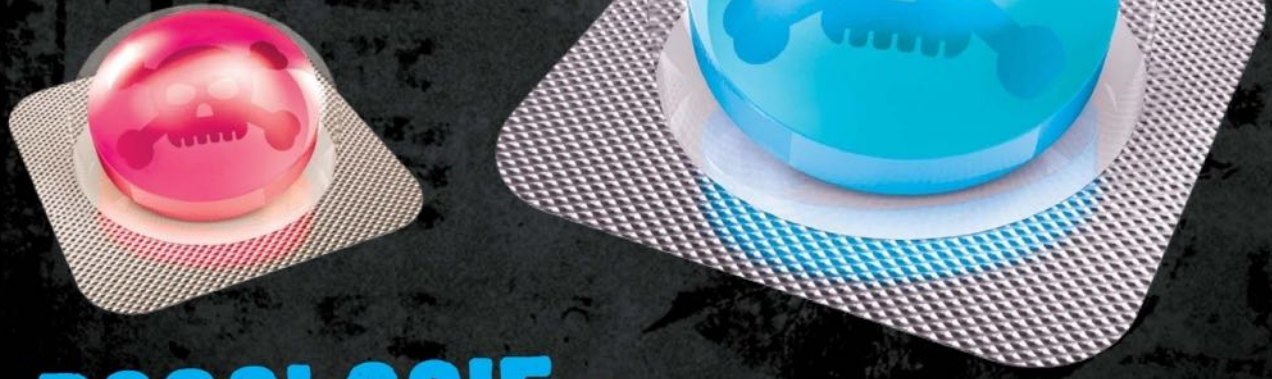
Si vous n'êtes pas très patient, mais que malgré tout, les Farmville-like vous intéressent, nous avons la solution. GMD Speed Time Lite se charge d'accélérer l'horloge interne de votre appareil pour flouer les jeux et leur faire croire que le temps avance plus vite. Dans la version gratuite, vous pouvez accélérer jusqu'à 10 fois. Attention, ne fonctionne pas avec tous les jeux (Clash of Clans, par exemple). À tester sur votre œuvre vidéoludique favorite.

https://goo.gl/fCE7xu

DANS CE MAGAZINE :

+ DE 80 TUTOS & ASTUCES

EN - DE 5 MN CHRONO !



L 14376 - 11 - 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 - NCAL/S : 620 CFP - POL/S : 660 CFP

POSOLOGIE :

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