# 5 étapes simples pour protéger vos smartphones *Android*

TrendLabs

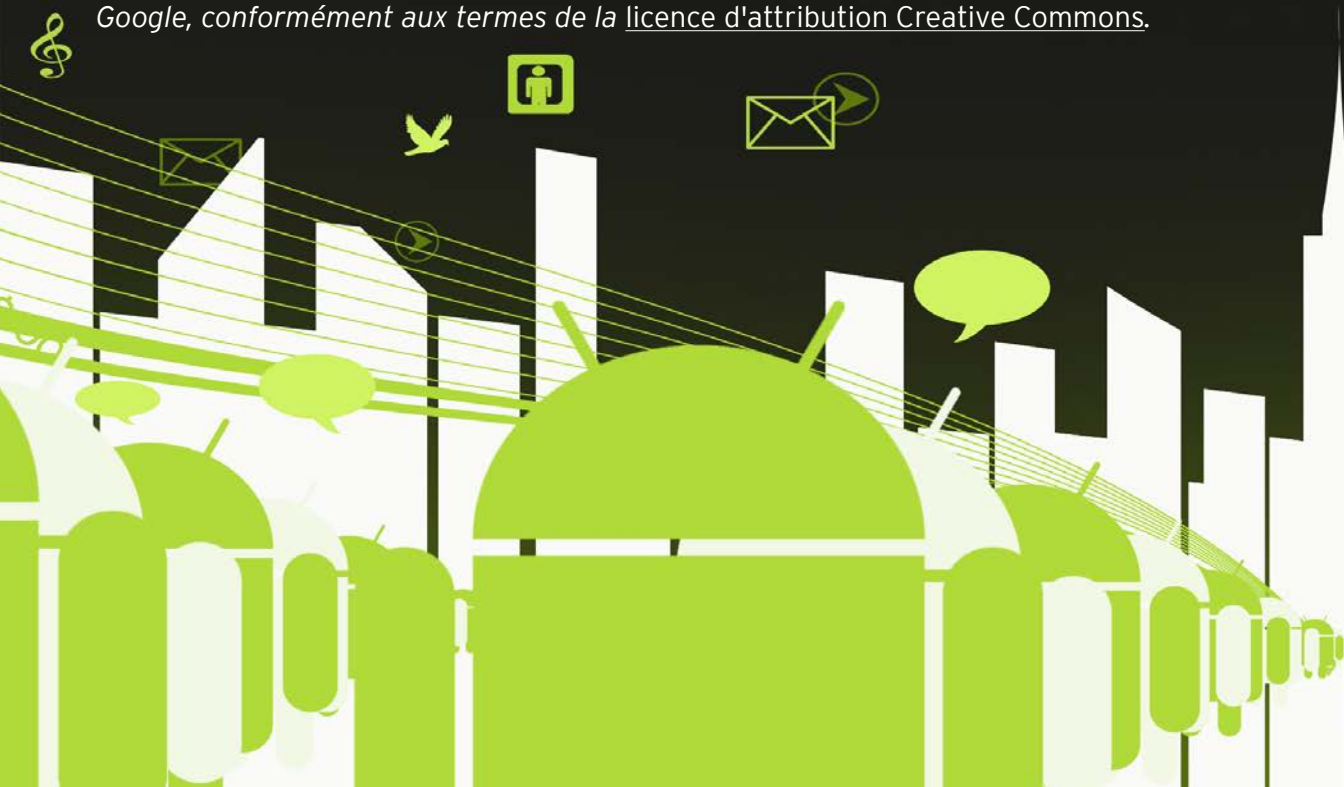
Global Technical Support & R&D Center of TREND MICRO

La plateforme *Android* de Google, fonctionnant sous la forme d'un logiciel libre refait rapidement son retard sur les systèmes d'exploitation *iOS* d'Apple et *BlackBerry OS* de RIM et compte de plus en plus de fidèles adeptes. Plafonnant à quelque 6,8 millions d'unités en 2009, les ventes mondiales de smartphones fonctionnant sous *Android* ont atteint le chiffre considérable de 67 millions fin 2010.

Au vu de la croissance des chiffres de vente, il ne fait aucun doute que l'« ère *Android OS* » connaît une ascension fulgurante. Tout le monde recherche un smartphone doté non seulement de fonctionnalités basiques de communication et d'envoi de messages, mais également de fonctions plus avancées d'un point de vue technologique. Qu'elles soient destinées à un usage professionnel ou récréatif, les applications pour smartphones *Android* ont rendu cette volonté possible.

---

** Le robot Android apparaissant dans ce livre électronique a été mis à disposition par Google, conformément aux termes de la licence d'attribution Creative Commons.*



L'une des caractéristiques les plus intéressantes du système d'exploitation *Android OS* est qu'il offre la possibilité aux développeurs de concevoir leurs propres applications innovantes et riches en contenu. Plus de 130 000 applications sont disponibles sur l'*Android Market* pour des utilisateurs présents dans 48 pays. La majorité de ces applications peuvent être téléchargées gratuitement, ce qui expose malheureusement certains utilisateurs à des risques, en particulier ceux qui téléchargent et essaient tous types d'applications. Il est en effet monnaie courante de voir des cybercriminels infecter les applications avec des chevaux de Troie pour s'enrichir.

Le fait que les applications *Android* soient également disponibles dans des boutiques tierces et sur le site des développeurs comporte d'autant plus de risques que cette réalité n'a pas échappé aux cybercriminels.

Avec toutes les données précieuses que renferme votre smartphone, vous devriez faire en sorte de le protéger contre toutes les menaces. Voici quelques conseils qui vous aideront à optimiser les paramètres de sécurité de votre smartphone *Android*.

# 1 Utilisez les paramètres de sécurité intégrés dans votre smartphone *Android*.

Le moyen le plus efficace de protéger votre smartphone consiste à configurer correctement les paramètres de localisation et de sécurité. Pour ce faire, accédez à l'option *Localisation & sécurité* dans *Paramètres*.

Il est également recommandé d'utiliser les fonctionnalités de verrouillage de base de votre smartphone, à savoir par le verrouillage par code PIN (numérique) ou par mot de passe. Si le fait de saisir votre mot de passe pour le déverrouiller peut vous sembler pénible, sachez que cela contribue à protéger vos données lorsque vous égarez votre téléphone.

Si cela n'est pas suffisant, vous pouvez utiliser l'option de verrouillage par empreintes digitales. Il s'agit vraisemblablement de la meilleure option, car elle garantit que vous êtes le seul à pouvoir accéder aux données stockées dans votre smartphone.

Rappelez-vous qu'il est toujours préférable d'utiliser l'une des options de sécurité précitées : mieux vaut prévenir que guérir ! Après tout, les mots de passe sont créés pour dissuader les cybercriminels d'accéder à vos données.

# 2 Désactivez l'option de connexion automatique aux réseaux Wi-Fi.

En plus de configurer correctement les paramètres de localisation et de sécurité de votre smartphone *Android*, il peut être utile de désactiver l'option de connexion automatique aux réseaux sans fil malgré son côté pratique.

Il existe plusieurs raisons de douter de la sécurité lors de l'utilisation d'un accès Internet sans fil gratuit. Simple, gratuite et pratique, la connexion à un réseau non sécurisé peut toutefois comporter certains risques. Accéder automatiquement à des réseaux sans fil non sécurisés revient à laisser la voie libre à n'importe qui. Les données stockées sur votre smartphone circulent librement sur le routeur ou le point d'accès sans fil et vice-versa. Ainsi, n'importe qui sur le même réseau peut consulter des informations que vous ne souhaiteriez pas divulguer.

Les utilisateurs de smartphones *Android* peuvent être confrontés aux mêmes menaces que celles auxquelles sont exposés les utilisateurs de PC. Cela concerne les risques associés à la connexion automatique à des réseaux sans fil, en particulier aux réseaux insuffisamment protégés. Ainsi, la désactivation de l'option de connexion automatique des réseaux sans fil constitue un autre moyen de se protéger des menaces mobiles.

# 3 Pensez à bloquer les applications provenant de boutiques autres que l'*Android Market*.

Le premier cheval de Troie sur *Android* se faisait passer pour l'application *Windows Media Player*. Peu après, un nouveau cheval de Troie sur *Android* a été détecté sur certaines boutiques d'applications tierces basées en Chine. Bien qu'il soit impossible de garantir l'intégrité des applications disponibles au téléchargement sur l'*Android Market*, on peut supposer que la boutique d'applications officielle est plus fiable que les autres.

Par conséquent, nous vous recommandons vivement d'utiliser l'option interdisant l'installation d'applications non issues de l'*Android Market*. Cela constituera une couche de protection supplémentaire pour votre smartphone.

# 4 Assurez-vous de bien comprendre les autorisations que vous donnez avant de les accepter.

Après analyse d'applications *Android* malveillantes, nous nous sommes rendu compte que celles-ci vous demandent généralement de les autoriser à accéder à une longue liste d'informations stockées sur votre smartphone. Parmi ces applications figure une version infectée par un cheval de Troie d'*Android Market Security Tool*, découverte récemment. Celle-ci demandait l'autorisation d'envoyer des messages texte vers des numéros surtaxés, de vous localiser, de consulter vos messages texte enregistrés et de modifier vos paramètres système. Le fait de donner votre autorisation lui permet d'agir comme une porte dérobée. Le programme rassemble et envoie les informations contenues dans le dispositif vers un URL à distance. Il exécute également d'autres fonctions sans votre autorisation, telles que la modification de vos journaux d'appels, la surveillance et/ou l'interception de vos messages texte et le téléchargement de vidéos.

Soyez vigilants lorsque vous acceptez des demandes d'informations personnelles et/ou relatives au dispositif ou d'autres actions non indispensables au fonctionnement d'une application. Réfléchissez à la manière dont une application souhaite fonctionner. S'il ne s'agit pas d'une application de répertoire téléphonique par exemple, elle n'a pas besoin d'accéder à votre liste de contacts.

# 5 Pensez à investir dans une application de sécurité mobile efficace.

Parfois, être vigilant lors du téléchargement ou de l'installation d'applications ne suffit pas. Étant donné que les cybercriminels ne se lasseront jamais d'inventer des méthodes ingénieuses pour vous amener à transmettre des informations personnelles, vous feriez mieux d'utiliser une solution de sécurité efficace.

Pour rester protégé n'importe où et à tout moment, vous pouvez compter sur des solutions telles que *Trend Micro™ Mobile Security for Android™*. Cette solution protège les fichiers numériques que vous stockez et sécurise les transactions bancaires que vous effectuez sur votre smartphone *Android*. Elle identifie et bloque les programmes malveillants avant même qu'ils n'atteignent votre téléphone. Vous avez ainsi l'esprit tranquille. Cette solution de sécurité complète s'appuie sur les technologies Trend Micro d'évaluation de la réputation de la messagerie et des sites Web pour protéger efficacement votre téléphone contre les toute dernières menaces mobiles.

Pour en savoir plus sur les dernières menaces visant les dispositifs mobiles *Android*, notamment les smartphones, lisez nos publications dans :

21:00

## Blog sur les programmes malveillants des TrendLabs

- Un outil de sécurité infecté par un cheval de Troie utilisé comme porte dérobée (angl.)
- Une application infectée par un cheval de Troie s'infiltre dans les dispositifs *Android* (angl.)
- RSA 2011 : la sécurité mobile dans le paysage actuel des menaces (angl.)
- La « consumérisation » de l'informatique mobile : risques et avantages (angl.)
- Un programme malveillant *Android* se propage via des boutiques d'application tierces (angl.)
- Une application *Android* malveillante localise les utilisateurs (angl.)
- Le premier cheval de Troie pour *Android* circule (angl.)

## TrendWatch

- **Clip sur la sécurité :** Paysage du mobile : risques de sécurité et opportunités (angl.)
- **Clip sur la sécurité :** Les téléphones portables sont les cibles de menaces de sécurité (angl.)
- **Clip sur les menaces Web :** Une porte dérobée se fait passer pour un *outil de sécurité de l'Android Market* (angl.)

## Encyclopédie des menaces

- **Article sur les attaques Web :** Des applications piratées affectent les utilisateurs du système d'exploitation Android (angl.)

**TREND MICRO™**

Trend Micro Incorporated est une société pionnière dans les domaines de la sécurisation des contenus et de la gestion des menaces. Fondée en 1988, Trend Micro offre aux particuliers et aux entreprises de toutes tailles des solutions logicielles et matérielles, ainsi que des services de sécurité primés. La société, dont le siège social se situe à Tokyo, est présente dans plus de 30 pays et ses solutions sont distribuées dans le monde entier par l'intermédiaire d'un réseau de revendeurs et de prestataires de services à valeur ajoutée. Pour obtenir de plus amples informations et des copies d'évaluation des produits et services Trend Micro, consultez notre site Web à l'adresse suivante : www.trendmicro.com.

**Trend Micro France S.A.**
85, avenue Albert 1er
92500 Rueil Malmaison

Tél. : +33 (0) 1 76 68 65 00
Fax : +33 (0) 1 76 68 65 05

**www.trendmicro.com**