

Maj 26 avril 2013

Préambule

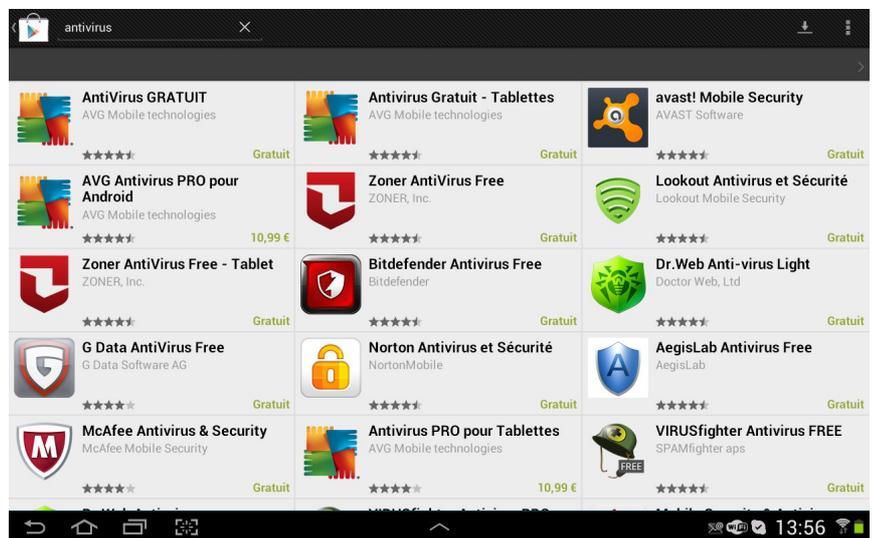
Comme tout système informatique, il est nécessaire de sécuriser l'environnement de travail sous Android. Ceci pour plusieurs raisons :

- Protection contre les virus.
- Verrouillage du système pour éviter les opérations de maintenance.
- Protection des données personnelles (mot de passe, carte bancaire...)
- Protection des mineurs

Antivirus

Les systèmes Android, représentant 75% des appareils mobiles, sont de plus en plus touchés par les virus. Ils peuvent causer le blocage du système, surfacturation téléphonique (dans le cas d'un appareil 3G), vol de données...

Il existe à ce jour des solutions de protection sous forme d'applications. Les plus grands éditeurs d'antivirus (payants ou gratuits) sont représentés (Avg, Avast, Bitdefender, McAfee...)



D'une manière générale, on installe l'application, on choisit les protections à activer et l'on sécurise l'application par un mot de passe.

Application de Verrouillage

Par défaut, les applications et paramètres système sont accessibles à l'utilisateur sous Android.

Il peut être intéressant de bloquer l'accès à certaines applications ou aux paramètres système dans un usage scolaire.

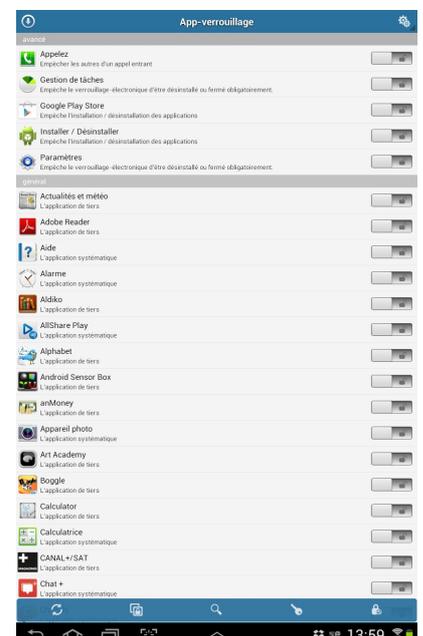
Pour ce faire, on utilise une application qui va fonctionner en tâche de fond. Elle demandera un mot de passe à chaque fois que l'utilisateur tentera d'accéder aux parties protégées par celle-ci.

APP de verrouillage fait partie de ce type d'application et est très simple d'utilisation.



Il suffit de définir le mot de passe puis de régler des curseurs pour définir le niveau d'accès.

Remarque : Certaines applications regroupent les fonctionnalités de verrouillage et d'antivirus en une seule.



Comptes et mots de passe

A partir du moment où les élèves ont à disposition des tablettes de prêt, il est au minimum nécessaire de :

- Mettre un mot de passe au compte google de gestion du play store connu uniquement des responsables de parc (et inconnu des élèves).
- Protéger le Google play store par un code PIN afin de bloquer l'accès aux applications à public restreint (adultes).



Dans le cas où il est décidé de ne pas bloquer l'accès au play store via une application de verrouillage, il faut être vigilant à l'usage des cartes bancaires : En effet, elles sont enregistrées dans le compte au premier achat... et profitent à tout le monde : Bien prévenir les familles avant le prêt. Ne pas oublier d'effacer la carte de l'établissement si elle a été utilisée ou utiliser des e-cartes bancaires à usage unique.

Protection des mineurs

Afin de respecter nos obligations légales, nous avons le devoir de mettre en place une protection des mineurs quant à l'usage des tablettes et des sites visités.

Cela ne pose aucun problème à l'intérieur de l'établissement scolaire à partir du moment où la connexion est réalisée à l'aide du réseau wifi établissement.

Par contre, il y a un problème lors de l'utilisation au domicile, depuis un wifi communautaire accessible depuis l'établissement ou via un partage de connexion depuis un téléphone mobile.

Diverses parades sont possibles :

- Limiter au seul usage depuis l'établissement scolaire en bloquant l'accès au menu "paramètres de la tablette"... Uniquement valable dans le cas où les tablettes restent dans l'établissement.
- Décharger la responsabilité sur les parents pour l'usage depuis le domicile... Mais pas de protection en cas d'accès via un téléphone ou via un réseau communautaire.
- Mise en place d'une application de contrôle parental tel que [Kaspersky Parental Control](#) en prenant soin, dans ce cas, de forcer l'utilisation du navigateur natif Android. ([article de référence](#)) Il faut donc penser à bloquer l'accès au navigateur Chrome également intégré aux tablettes.

Auteur

Hugues LAFFEZ, Animateur DANE
Hugues.laffez@ac-nice.fr