almerys

G2S - Group

Fleurance - Vendredi 3 juin 2016

La sécurité des terminaux mobiles

Selon le CLUSIF*, de nombreux freins existent dans la sécurité des terminaux mobiles :

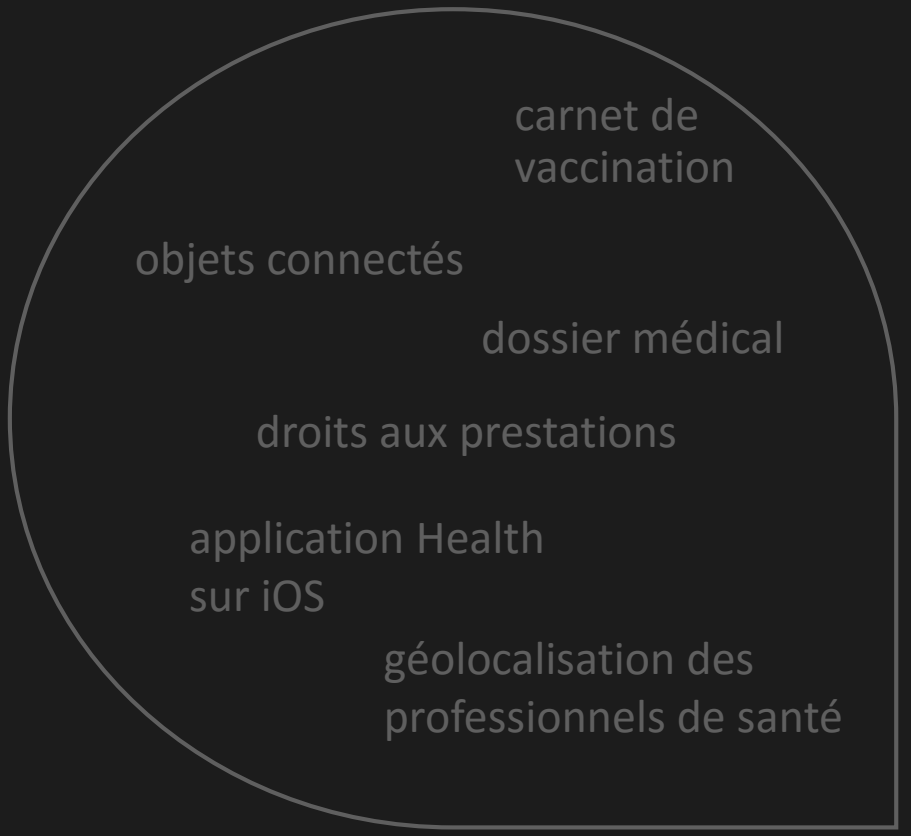
- une sensibilisation défaillante
- une négligence de l'aspect « ordinateur » de nos terminaux mobiles
- des malwares de plus en plus présents sur ce support
- un refus de toutes contraintes par les utilisateurs
- un marché qui ne propose pas vraiment de solutions permettant de sécuriser les terminaux mobiles
- …

*Club de la Sécurité de l'Information Français

Le voyageur et les données de santé

De plus en plus, d'applications permettent à **l'utilisateur nomade** de faciliter la gestion de sa santé

Ces applications sont particulièrement utiles lors des voyages



En pratique …

M. Z visite le parc naturel régional du Livradois-Forez

Il souffre d'insuffisance cardiaque et ne se sent pas bien. Il doit rapidement **trouver** :

Un cardiologue qui pratique le tiers payant avec sa mutuelle
Une pharmacie pour aller chercher son traitement

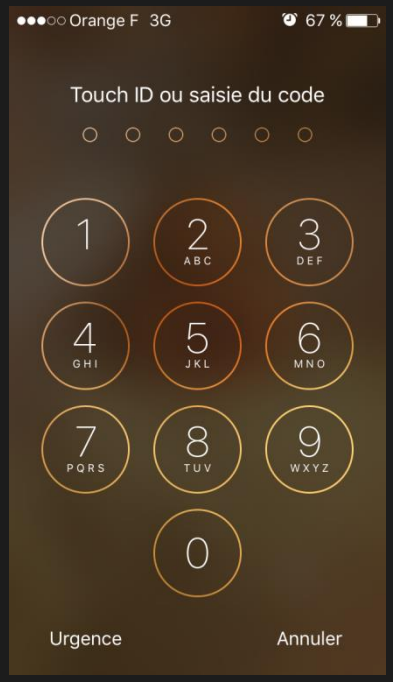
Il a à sa disposition une application qui lui permet :

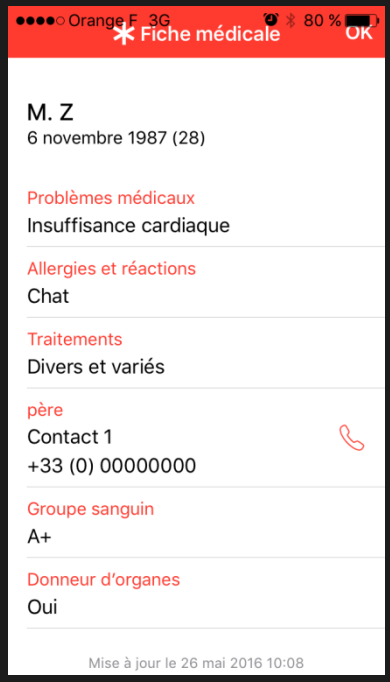
De géolocaliser les professionnels de santé autour de lui
De prouver ses droits de bénéficiaires

En pratique …

M. Z découvre le Gers et ses merveilles gastronomiques

Lors d'une promenade au soleil après un bon repas, il fait un malaise.
Les secouristes arrivent et découvrent que M. Z a un smartphone **sur lequel il est possible d'accéder aux informations médicales pour les urgences**





Les risques :

Les deux scénarios montrent des **risques de compromission de données sensibles** :

- Dans le premier cas l'utilisateur **ne choisit pas d'exposer les données** car il fait **confiance à des applications.**

- Dans le deuxième cas **l'utilisateur expose volontairement des données.** Ces données sont accessibles par n'importe qui **même sur un téléphone verrouillé**.

- **Dans tous les cas, si l'utilisateur a installé un malware** celui-ci peut **compromettre les applications qui traitent des données sensibles** et potentiellement **compromettre le SI qui les héberge** s'il est mal protégé.

Une protection par les fournisseurs d'applications :

L'identité numérique de l'individu doit être obtenue par le biais d'un enrôlement fiable.

L'identité numérique de l'individu qui accède à un système doit pouvoir être **vérifiée efficacement.**

Les données manipulées ne devraient jamais être stockées sur le terminal mais uniquement dans **des centres de données sécurisés.**

Tout fournisseur d'applications qui manipulent des données de santé devraient avoir **un agrément HDS**.

Une protection qui passe par les autres acteurs :

Tous les acteurs doivent prendre conscience des problématiques de sécurité, notamment autour des données de santé.

Le professionnel de santé devrait être a minima identifié pour accéder au terminal d'un tiers.

L'utilisateur ne devrait pas:

- Installer n'importe quoi sur son smartphone
- Provoquer de situation où il met de lui-même en péril ses données personnelles