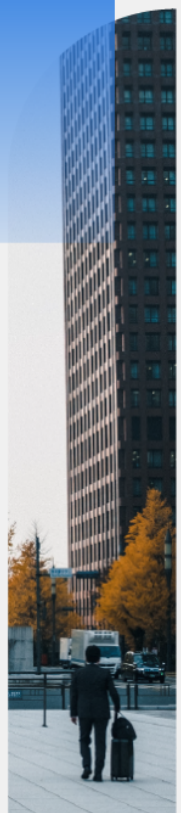


Touche pas à mon dossier médical !

Axelle Apvrille

SecSea, La Ciotat, Octobre 2021

Bonjour ! Qui suis-je ?

- **Principal Security Researcher** chez **Fortinet**
- Thèmes: Malware sur Android et IoT
- Ph0wn CTF, 3 décembre 2021 à Sophia Antipolis
- Email: aapvrille (at) fortinet (dot) com
- Twitter: @cryptax

Hospital ransomware attack caused baby's death by shutting down heart rate display, lawsuit claims

Lawyers for Teiranni Kidd accused Springhill Hospital in Alabama of negligence over the 'preventable' death of her daughter Nicko during a cyberattack

Independent Staff | 3 days ago | 1 comments

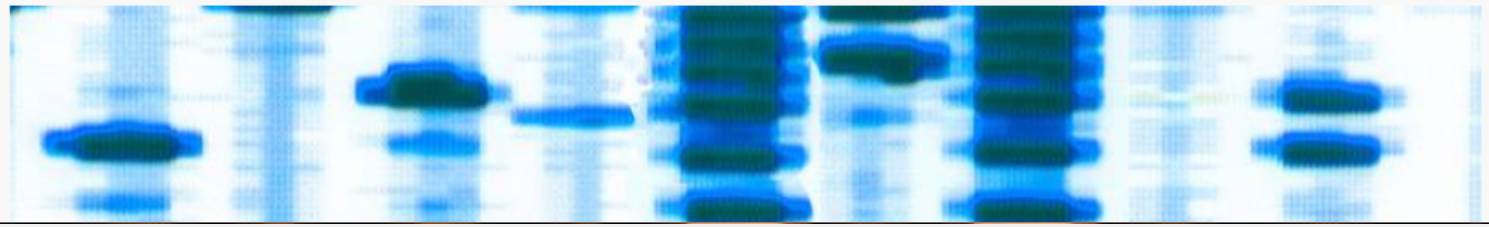
Source: Independant.co.uk, 1er oct 2021

Info Libé

Les informations confidentielles de 500 000 patients français dérobées à des laboratoires et diffusées en ligne

Article réservé aux abonnés

Selon les spécialistes, la fuite est d'une ampleur inédite en France pour des données ayant trait à la santé. Le fichier en question, que «CheckNews» a pu consulter, contient l'identité complète de près d'un demi-million de Français, souvent accompagnée de données critiques, comme des informations sur leur état de santé ou même leur mot de passe. Initialement partagée sur des forums de pirates informatiques, cette base de données est de plus en plus largement diffusée.

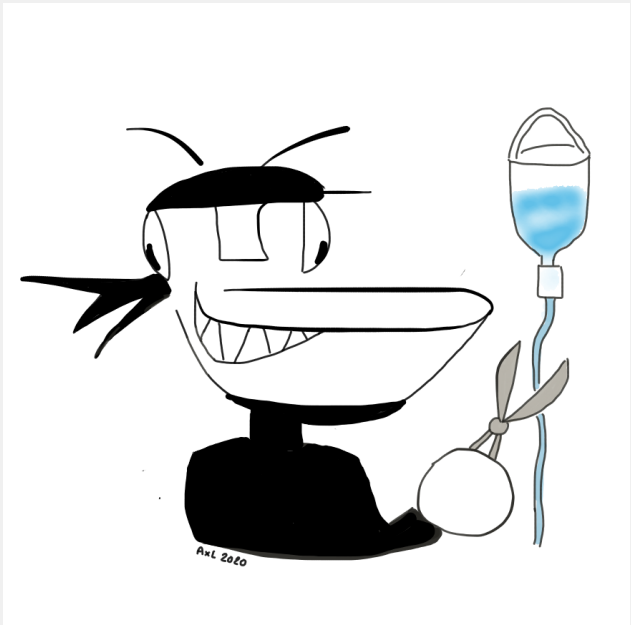


Source: Libération, 23 fév 2021

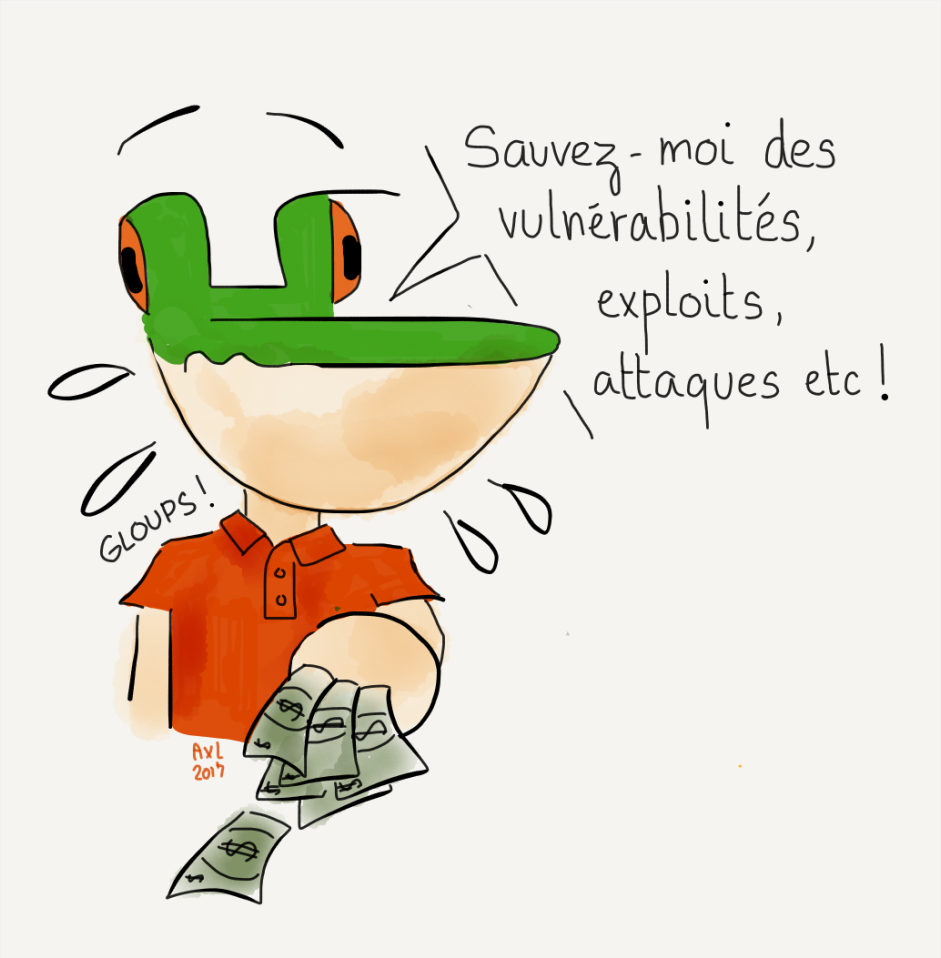
La sécurité de nos données médicales est-elle vouée à l'échec ?

Complexité du milieu médical

- Beaucoup de matériel différent.
- Sécurité physique des appareils difficile à garantir.
- Personnel médical, administatif et patients avec peu (ou pas) de *connaissances en sécurité informatique* et/ou peu (ou pas) *de temps*.



Donc, c'est fichu ?



4 exemples du milieu médical

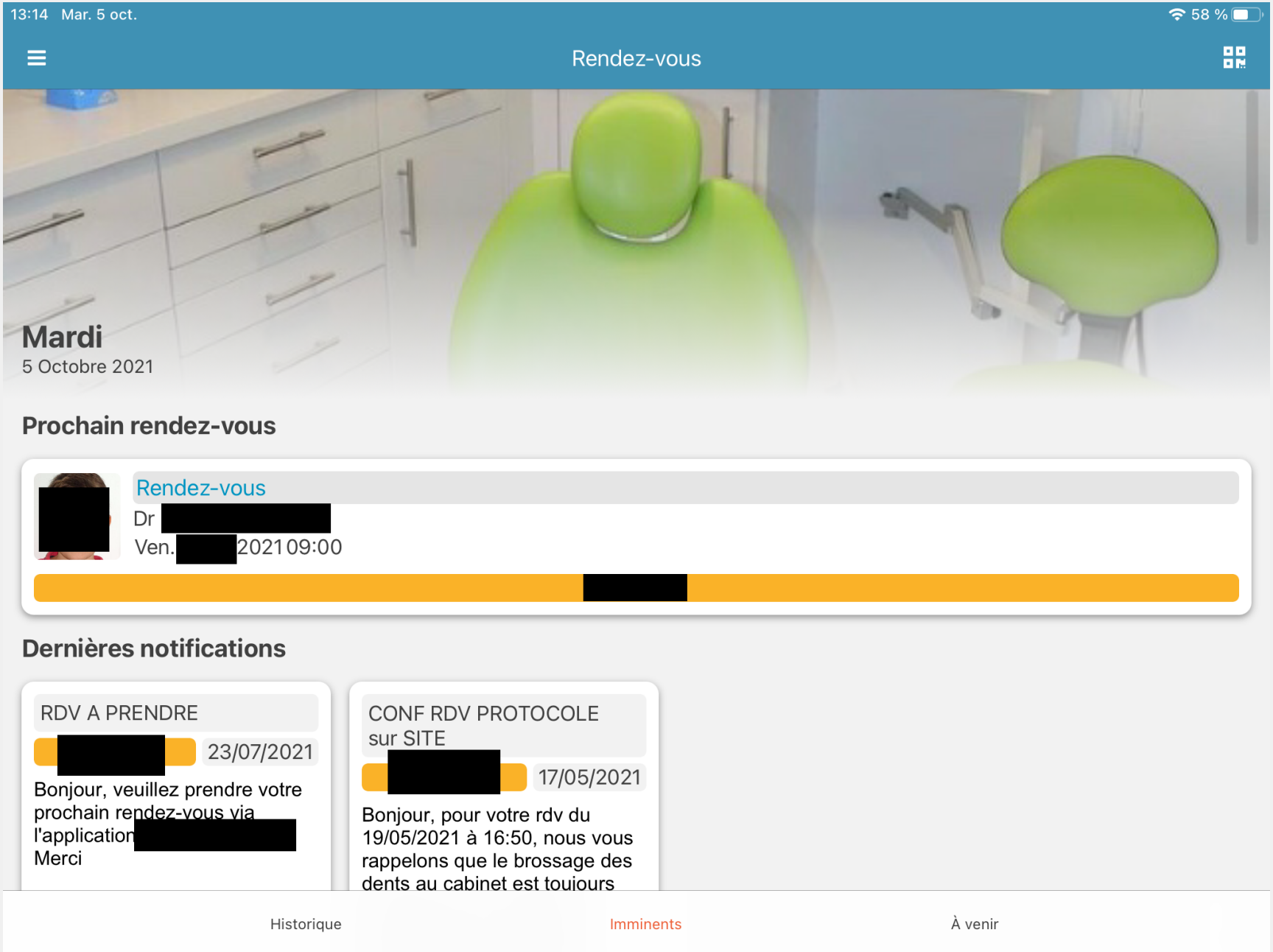
- Cabinet d'orthodontie
- Laboratoire d'analyse
- Vaccination COVID
- Ophtalmologie

- Faille(s) de sécurité évidente(s). **Pas dignes de 2021**.
- Solution: je cherche une solution **à moindre effort**. Hélas pas parfaite.

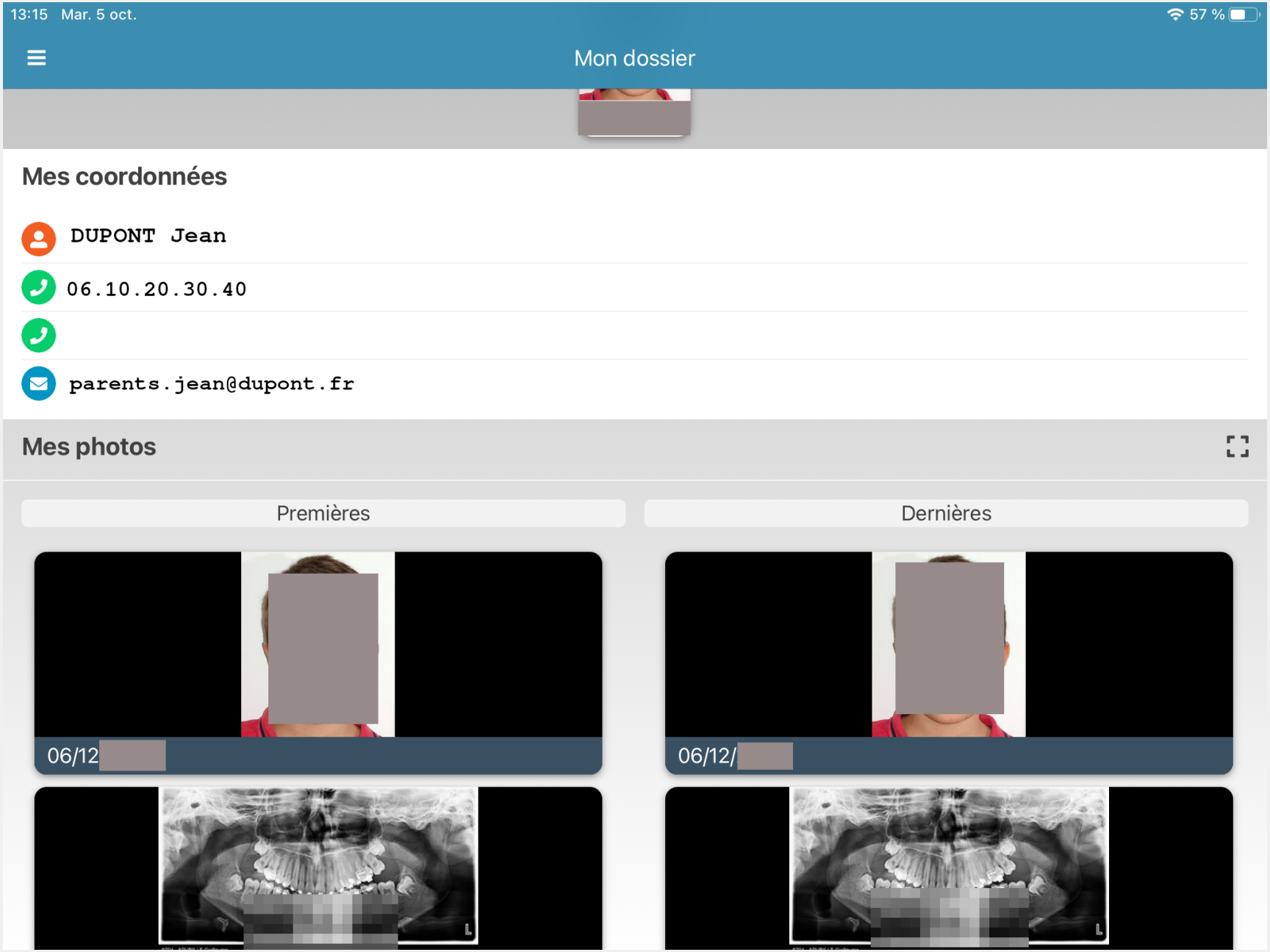
EXEMPLE 1

Cabinet d'orthodontie

Cabinet d'orthodontie



Cabinet d'orthodontie



Création de compte

Afin de préparer le prochain rendez-vous de : [redacted] nous vous invitons:

• Télécharger gratuitement l'application [redacted] sur votre smartphone (sur le store de votre téléphone).

DISPONIBLE SUR App Store

Disponible sur Google play

Pour vous connecter:

Code du cabinet: 06100

Identifiant DUPONT1234

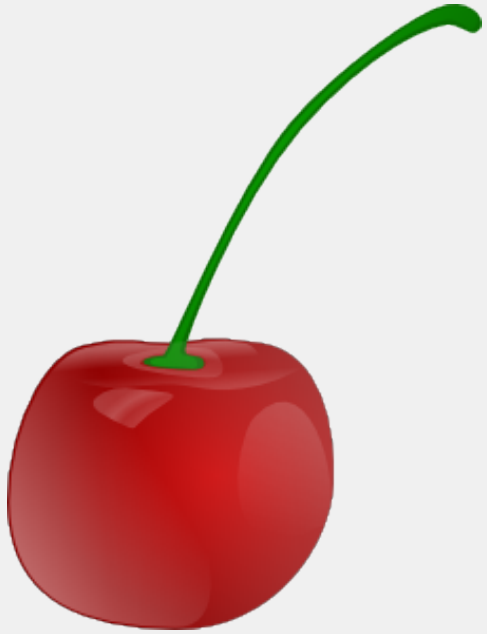
Mot de passe: 1234

ATTENTION : Si vous êtes **responsable légal de plusieurs patients suivis chez nous**, connectez-vous avec les identifiants suivants pour un accès au dossier de TOUTE la famille:

Identifiant: DUPONT12345

Mot de passe: 12345

Création de compte



On ne peut pas changer son mot de passe

Réponse du Directeur Technique: Couplet TLS

Sécurité des échanges

L'application [redacted] utilise le protocole TLS pour sécuriser le transport des informations, il s'agit d'une technologie standard dest protection des données sensibles qui sont transmises entre deux systèmes, empêchant les attaquants de lire et de modifier les inform informations personnelles.
De plus [redacted] respecte les contraintes imposées par la diffusion d'application mobile dans l'Apple Store et le Googe Play Store.

"L'application utilise le protocole TLS"

Réponse sur la “sécurité” du mot de passe

Extrait de l’email

“Les noms d’utilisateur / mots de passe sont-ils assez complexes ? Après s’être connecté à un cabinet, le patient doit se connecter à son profil Internet, ce profil est accessible depuis la fichier du patient XXX, si le schéma automatisé ne convient pas le mot de passe peut être changé depuis XXX = POSTE DU CABINET. Nous envisageons d’ajouter la possiblité de changer le mot de passe par le patient lui-même”.

Invraisemblable !!!

Bilan

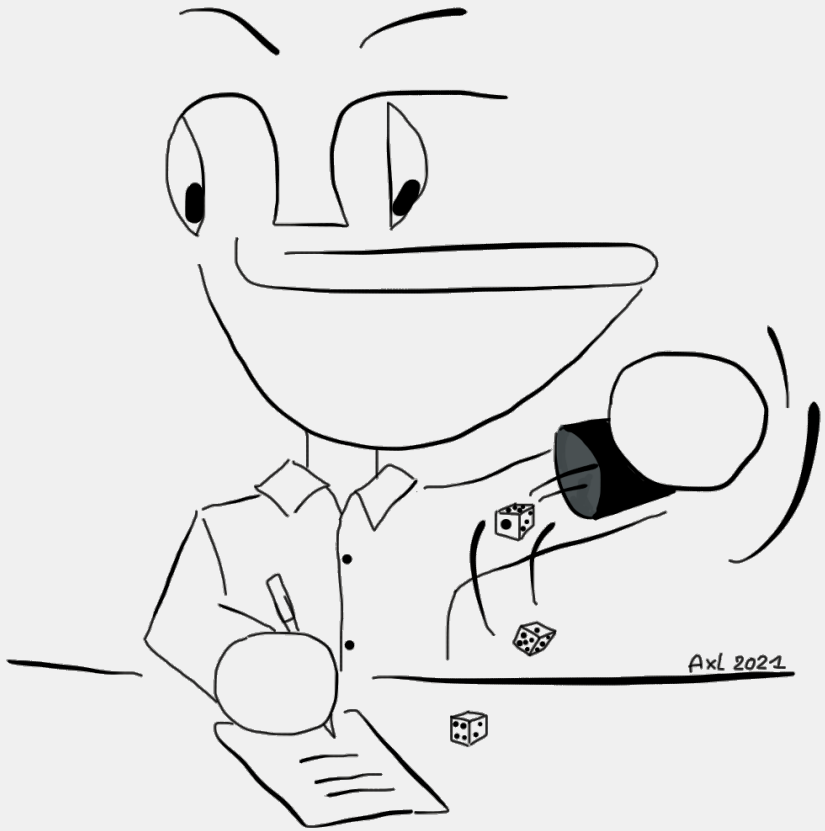
Positif

- Le cabinet d'orthodontie a pris ma requête au sérieux ✌
- Le directeur technique a pris le temps de faire une réponse détaillée. *Mais il n'améliore pas la sécurité de son application*.
- Je peux accéder aux panoramiques dentaires de mes enfants sans avoir à les demander.

Négatif

- L'application ne me simplifie pas la vie
- Utilité ? A débattre
- Les **cybercriminels peuvent obtenir les panoramiques dentaires de mes enfants, nom, prénom, age, photo, téléphone des parents, adresse** etc.

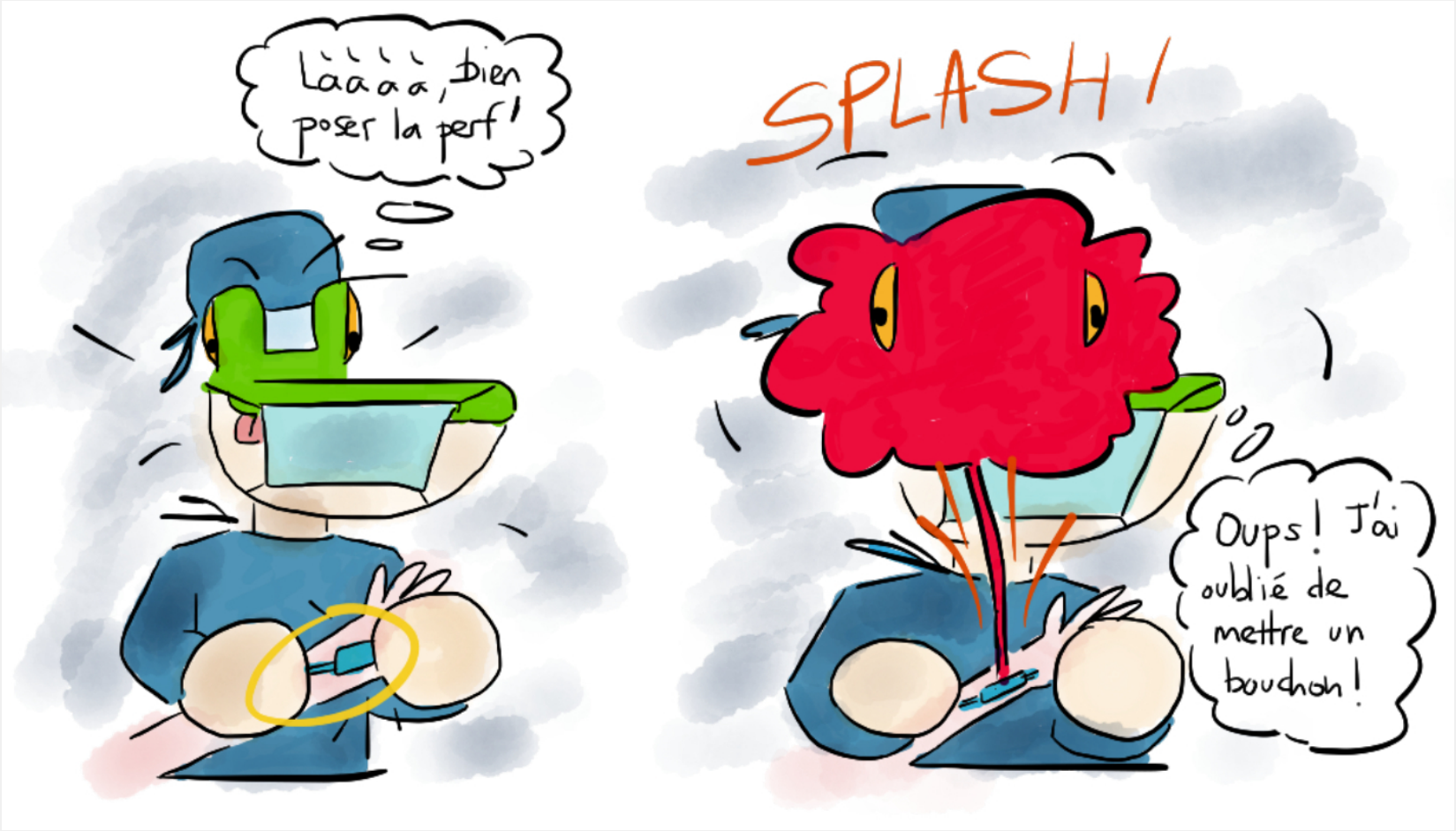
Recommandation 1



Générez les mots de passe aléatoirement

\+ forcer le changement à la première connexion

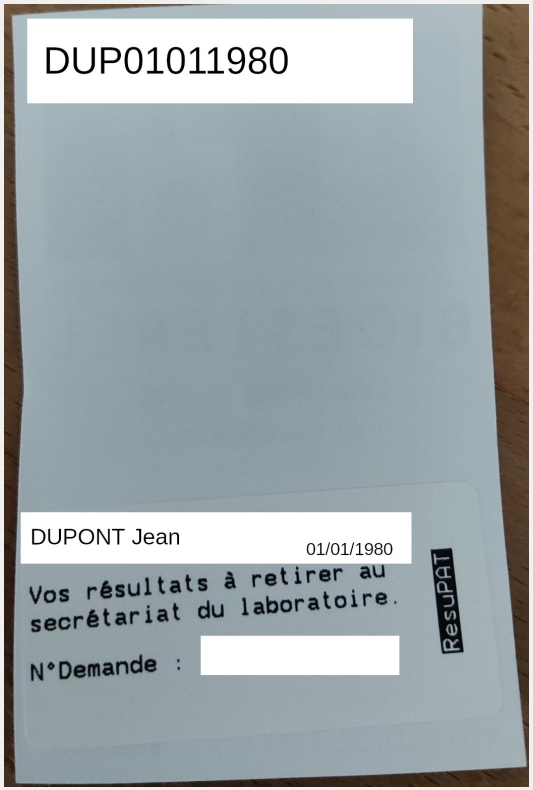
*Il faudrait aussi utiliser un canal sécurisé pour transmettre le mot de passe, ou double authentification etc



EXEMPLE 2

Résultats d'analyses médicales

Accès aux résultats d'analyse 1/3



Mot de passe : 3 premières lettres du nom de famille + date de naissance

Accès aux résultats d'analyse 2/3

LABORATOIRE [redacted]

[redacted]

Bonjour [redacted],

Vous avez souhaité recevoir vos résultats d'examens à cette adresse e-mail.

Veuillez trouver en pièce jointe le compte-rendu de vos analyses du [redacted]-2021.
Un mot de passe vous sera demandé pour ouvrir le fichier PDF joint, celui-ci vous a été communiqué au laboratoire lors de votre prélèvement.

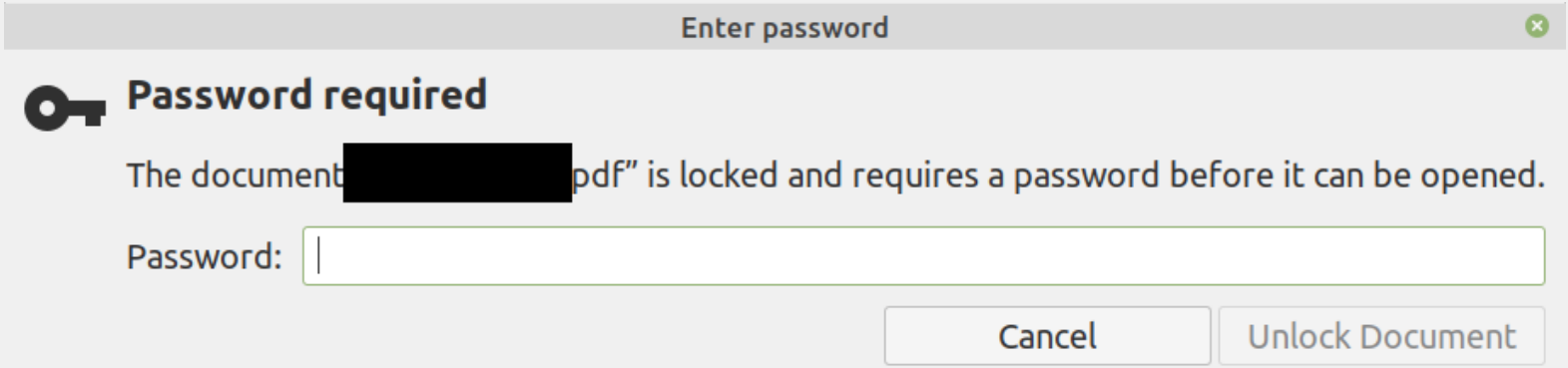
Nous vous remercions pour votre confiance et vous invitons à prendre quelques secondes pour nous donner votre avis. Votre avis est important. Il nous permet de nous améliorer et vous permet d'encourager nos équipes.

ETES-VOUS SATISFAIT DE VOTRE PASSAGE DANS NOTRE LABORATOIRE ?

OUI NON

L'inscription à ce nouveau service ne modifie en rien vos habitudes. Les résultats de vos examens seront

Accès aux résultats d'analyse 3/3



Accès aux résultats d'analyse 3/3

Dossier [redacted] –2021 [redacted] né(e) [redacted]

Intervalle de référence *Antériorités*

MICROBIOLOGIE

Détection du génome du SARS CoV–2 par RT–PCR (Covid19)

MGI Easy Extraction for Viral DNA RNA by Magnetic Beads / Elitech SARS–CoV–2 ELITe MGB
(changement de technique à partir du 09/11/2020)

Lieu de réalisation de l'analyse	Plateau technique [redacted]
Origine du prélèvement	Naso–pharyngé
RdRP gene	Négatif
ORF8 gene	Négatif
Conclusion :	**SARS–CoV–2 négatif : absence de détection de l'ARN viral** *Negative SARS–CoV–2: absence of detection of viral RNA*

Le kit de RT–PCR utilisé détecte l'ARN viral des différents variants de Covid, y compris les variants du Covid en provenance du Royaume–Uni (variant VOC 202012/01) et d'Afrique du Sud (variant 501.V2). Selon les directives de la DGS, à partir du 25 Janvier 2021, tout résultat de PCR positive fait l'objet d'un criblage à la recherche des variants UK et brésilien/sud–africain. Le cas échéant, un compte rendu complémentaire vous sera adressé par mail.
Selon Santé Publique France, nouvelle stratégie de freinage à compter du 22 Février 2021 :

Pas besoin d'artillerie lourde

4 secondes

Si on connait votre nom de famille, il faut 4 secondes pour casser le mot de passe

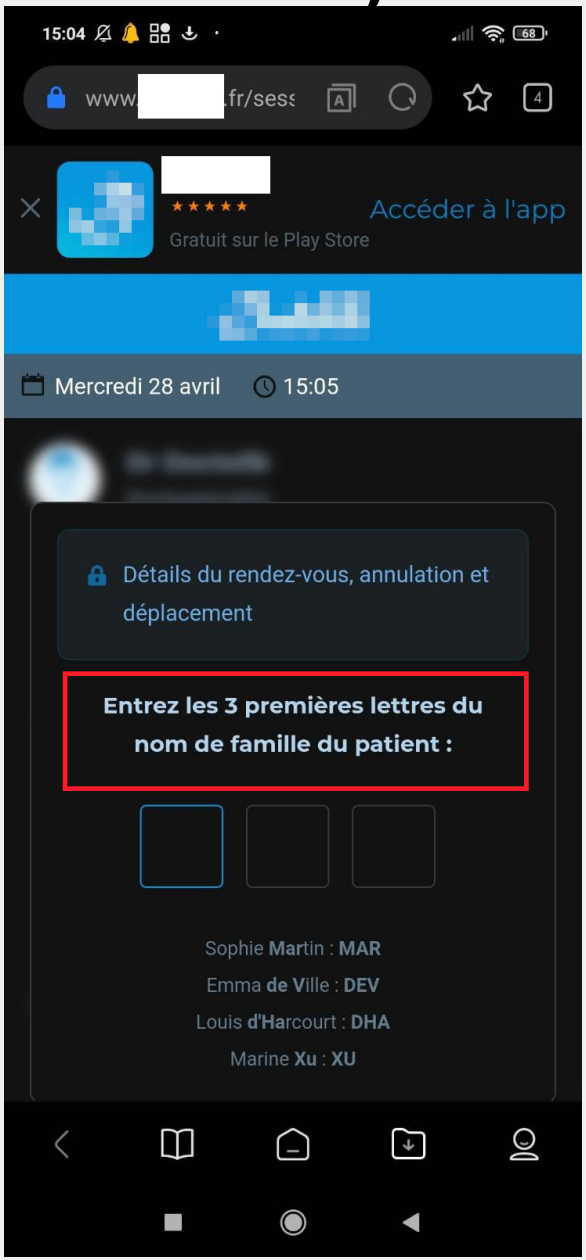
Recommandation 2

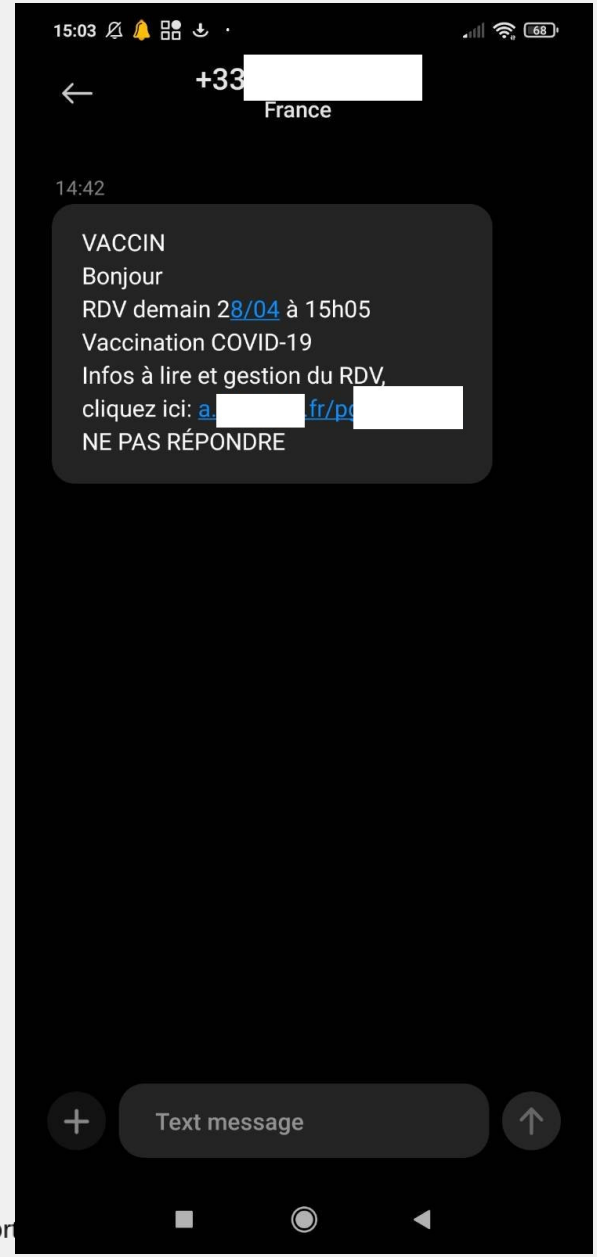
- Double authentification: **mot de passe aléatoire** + **SMS**. **Solution de repli**: si le patient n'y arrive pas : aller chercher ses résultats au laboratoire (certains préfèrent, quoi qu'il arrive).
- Accès via la carte Vitale ?

EXEMPLE 3

Rendez-vous vaccination COVID19

Rendez-vous vaccination (ou annulation, déplacement...)





Recommandation 3

Générez les mots de passe aléatoirement

- La population qui sait manier appli et SMS sur smartphone **sait aussi gérer des mots de passe aléatoires**
- Double authentification ?

*Aucune solution n'est parfaite

EXEMPLE 4

Ophtalmologie

Toutes les informations sont issues de documentations **publiques** sur **Internet**

HD OCT / Imagerie microscopique et tomographique haute résolution

Aide au diagnostic :

- Trous maculaires
- Rétinopathie
- DMLA
- Glaucome
- ...

Log On to Windows

The Model 500 and 5000 instruments are configured to automatically log on to Windows and start the CIRRUS application. Automatic log on is performed using the **Zeiss** user account and the following password:

November171846

The password (representing the founding date of the Carl Zeiss company) is case-sensitive and has no spaces.

Source : documentation publique, officielle du logiciel (page 4) et matériel (page 31)

Autres perles

Note: To preserve system access, optimum system configuration, and networking capabilities, do not change the default Windows user account and password.

Note: Do not edit nor delete the **Tech Support** account, which is used only by ZEISS technical support personnel. If you change or delete this account, CZM technical support may be unable to restore access to your system, in case you lose the password for the Administrator account. In this case, a service call would be required to replace the system hard drive.

Manuel utilisateur du HD-OCT (page 32) - public

1. Mauvais conseil informatique
2. Présence d'une porte dérobée

Humphrey Field Analyzer / Analyseur de champ visuel

Aide au diagnostic :

- Glaucome
- Troubles neurologiques
- Défauts de champs visuels

Installing HFA Review

Note: The User Type drop-down box will initially be blank, but once you select a user type, HFA Review will remember it for the next time you log into the application.

5. Type in the default password, which is four zeros: 0000. Zeiss recommends that you change your password after logging in for the first time.
6. Click **Login** when done. The PATIENT screen appears.

Mot de passe par défaut: **0000**

Source : documentation publique et officielle du logiciel (page 14) et du matériel.

Recommandation 4

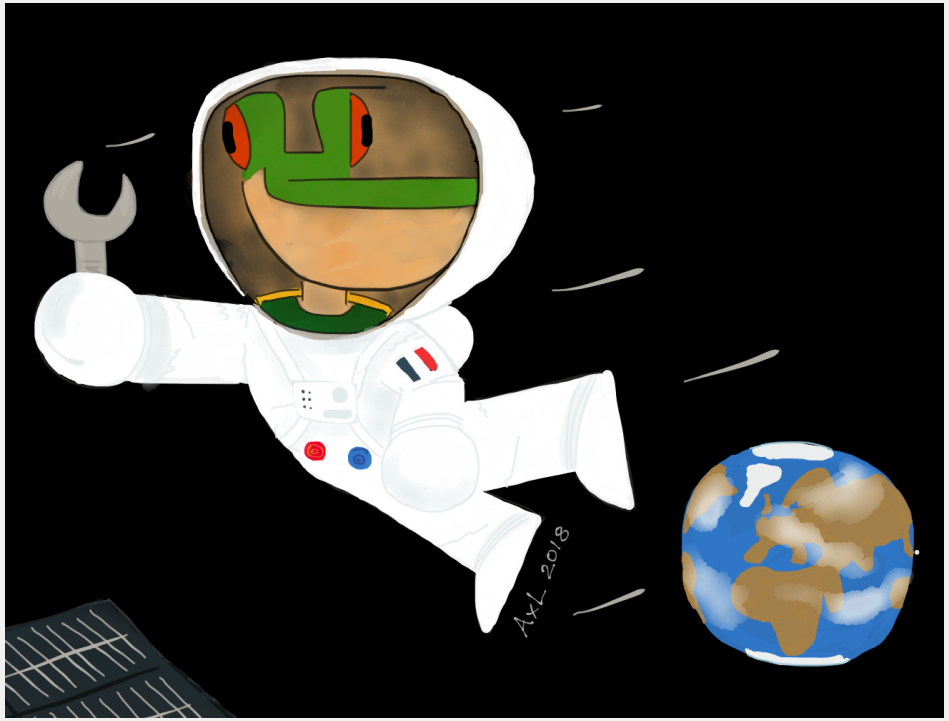
Forcer le changement de mot de passe à l'installation

*Aucune solution n'est parfaite

Que retenir ?

Si je laisse une boite ouverte, pleine de chocolats,
il y en a forcément qui se serviront

Un petit pas pour l'homme, un grand pas pour l'humanité



Révisez vos schémas de mots de passe

Recommandations finales

- Installez et tenez à jour un **anti-virus** en amont sur le réseau
- Demandez aux utilisateurs d'installer des **gestionnaires de mots de passe**
- Les applis, accès Internet, ce n'est pas fait pour paraitre "à la mode". Si vous ne savez pas sécuriser les données sensibles, *ne les mettez pas sur Internet* !
- **Corrigez les vulnérabilités** qui sont remontées et remerciez les chercheurs pour leur aide.


FORTINET