Rapport des bonnes pratiques de gestion des mots de passe.

# Conseils à appliquer :

Un conseil donné dans l’article que je devrais suivre et mettre en place est d’utiliser un mot de passe différent pour chaque service, surtout pour les plus importants. Un bon gestionnaire de mots de passe sera bien utile.

En effet, j’utilise différents mots de passe mais pas que des différents.

Ensuite, activer la double authentification à chaque fois que c’est proposé, même aller activer manuellement, serait une bonne chose à faire. J’utilise trop peu la double authentification.

Le gestionnaire de mots de passe *KeePass* est cité. Personnellement j’utilise déjà celui de Firefox (il ne propose de sauvegarder un mot de passe et identifiant lors d’une connexion/inscription. Travaillant sous Mac, MacOs propose également un gestionnaire de mots de passe nommé *Trousseau*. Ce service permet de générer un mot de passe très robuste (très long, caractères en minuscules/majuscules, …) et les sauvegarde au sein du système ou d’iCloud. Le service est assez pratique si on possède d’autre périphériques Apple d’après mon expérience. Cependant, je trouve que sauvegarder ses mots de passe dans le cloud et chez une grande firme comme Apple sois la meilleure chose en termes de confidentialité.

Ensuite, les mots de passe que j’utilise sont plutôt robustes selon les critères recommandés. Ils ne sont, forcément, pas devinables. Je ne me suis pas basé sur une méthode de conception comme cité dans l’article mais il est vrai que ce sont d’excellents moyens de créer des mots de passe.

Je n’ai jamais eu de soupçons sur la fiabilité ou le secret de mes mots de passe, j’ai également été voir sur un site s’ils n’ont pas fuité (même si ce n’est pas la meilleure chose à faire). J’évite les ordinateurs publics, partagés, etc. et quand je le fais (à HELMo, dans les labos) je n’enregistre jamais le mot de passe.

Enfin, le mot de passe par défaut donné par HELMo lors de mon inscription a immédiatement été changé.

# Procédure 2FA :

L’application que j’ai choisie est Twitter, voici la procédure de double authentification avec un code via l’application 2FAs :

1. Parcours dans les paramètres pour atteindre le service 2FA :

Une image contenant moniteur, écran, capture d’écran, route

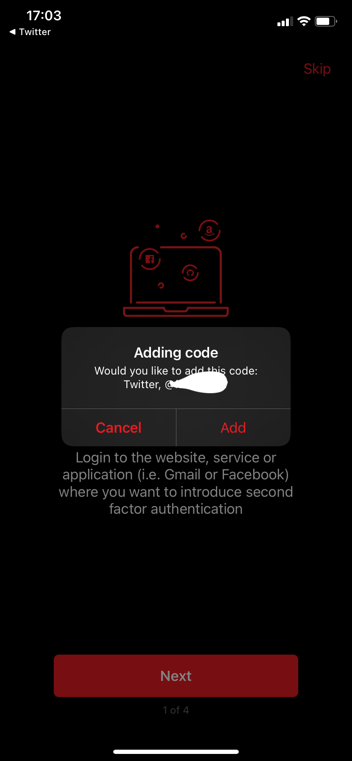
Description générée automatiquementUne image contenant texte

Description générée automatiquement

1. Choix d’utiliser l’application *2FAs* :

Une image contenant texte

Description générée automatiquementUne image contenant texte

Description générée automatiquement

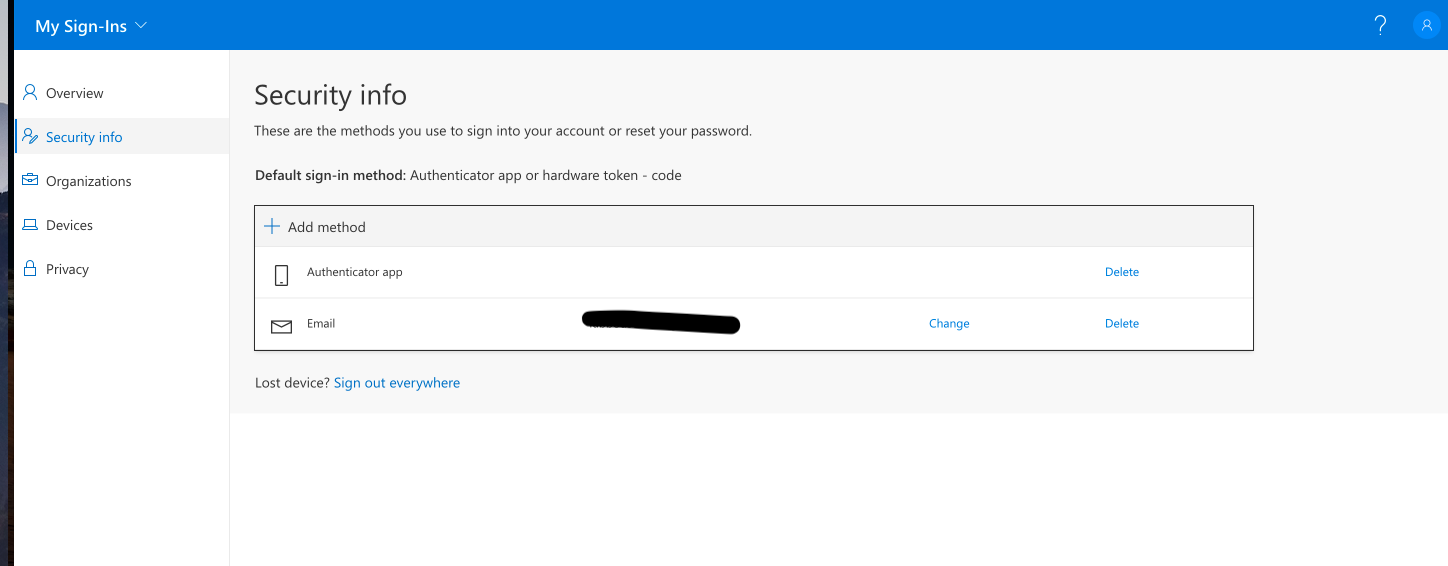
1. Connexion à mon compte Twitter :

Une image contenant ordinateur

Description générée automatiquementUne image contenant texte

Description générée automatiquement

# Procédure 2FA Microsoft HELMo :



# Authentification Windows 10 :

1. *Quels sont les dangers des comptes Microsoft ? Comment Microsoft a-t-il résolu ces risques de sécurité ?*

L’un des dangers est que les comptes Microsoft sont des comptes en ligne et donc par internet, ce qui veut dire que lorsqu’un utilisateur veut s’y connecter, il échangera avec un serveur. Une personne mal intentionnée pourrait donc intercepter les données échangées et les utiliser pour se connecter aux services Microsoft liés au compte.

Car le second danger est que le compte Microsoft donne accès à plusieurs services de Microsoft. Si un pirate a su prendre possession du compte, celui-ci aura accès à tous les services en ligne, sur PC ou sur smartphone de l’utilisateur (il pourrait lire les emails, des messages échangés, un agenda, …).

Afin de remédier à ces problèmes, Microsoft a mis en place des moyens d’authentification multiple : utilisation d’un code PIN, de la reconnaissance faciale, mot de passe par image, …

1. *Suite à cette lecture, quels sont les méthodes d'authentification que vous recommanderiez sur un Windows 10 ?*

Personnellement, je recommanderais d’activer l’authentification multiple, avec au moins 2 facteurs :

Premièrement, un mot de passe robuste avec les minimums 8 caractères, minuscules, majuscules, chiffres, caractères spéciaux.

Deuxièmement, le code PIN ou confidentiel est un excellent choix car ce code est local à la machine et il est chiffré. C’est un problème lorsque l’utilisateur souhaite accéder à son compte Microsoft depuis un autre appareil mais c’est très sécurisé pour l’ordinateur.

Ensuite, Windows Hello est un excellent facteur d’authentification car il faut être l’utilisateur et c’est aussi local. Il faut évidemment être à l’aise avec l’idée que ces données sont récoltées par Microsoft.

Enfin, je recommanderais une clé de sécurité physique (ou un générateur de clés sur un autre appareil) pour l’authentification aux applications Microsoft.

1. *Pourquoi le code PIN de moins de 6 caractères est-il plus sécurisant qu'un mot de passe sur Windows 10 ?*

Le code PIN est plus sécurisant pour plusieurs raisons.

D’abord, il est stocké localement à la machine et donc il ne peut pas être intercepté par une personne malveillante.

Ensuite, ce code est chiffré sur base des puces TPM. Cette puce est protégée contre des modifications et elle est disponible sur de nombreuses machines Windows 10.

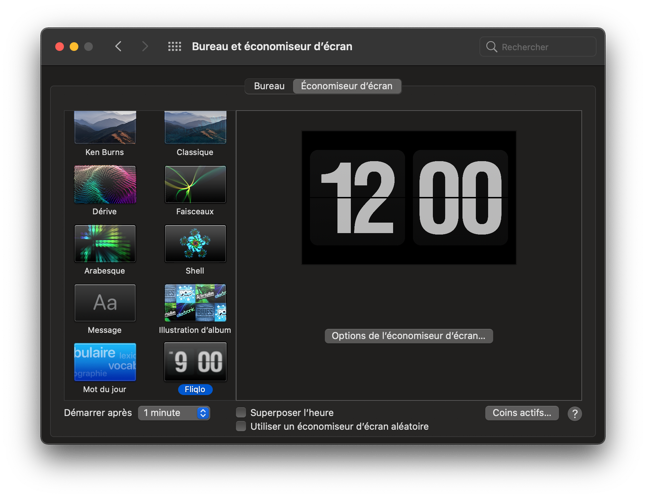
1. *Qu'est-ce que Windows Hello ? Tous les systèmes sous Windows 10 peuvent-ils l'utiliser et pourquoi ?*

Windows Hello est une méthode d’authentification par biométrie. L’utilisateur peut l’utiliser avec la reconnaissance faciale ou digitale et ne requiert aucun mot de passe.

Cependant, malgré que l’option soit disponible pour tout utilisateur de Windows 10, la machine doit avoir les composants hardware qui permettent d’authentifier l’utilisateur : une caméra de reconnaissance faciale et/ou un capteur d’empreinte digitale.

## 4.1 Procédure d’authentification MacOs :

### Une image contenant texte, capture d’écran, moniteur, noir Description générée automatiquement4.1.1 Programmer le verrouillage :



### 4.1.2 Sécuriser le PC avec un code PIN :

Pas de possibilité de mettre en place un code PIN.

### 4.1.3 Sécuriser le PC sans mot de passe avec Touch ID :

