Le MFA

Par Patrick Sentinel – 29a.ca

MFA pour les Nuls : comment arrêter de servir votre mot de passe sur un plateau d'argent aux hackers

Vous pensez que votre mot de passe **"P@ssw0rd123"** est incassable ? Vous êtes persuadé que personne ne devinera jamais **"querty2024"** ? Mauvaise nouvelle : **les hackers adorent les gens comme vous**.

Heureusement, il existe un moyen simple de **ne pas se faire pirater en 3 secondes** : l'authentification multi-facteurs, ou **MFA (*Multi-Factor Authentication*)**. Ça peut sembler technique, mais promis, c'est **aussi simple que de mettre un verrou sur sa porte d'entrée** (et sérieusement, qui laisse sa porte grande ouverte aujourd'hui ?).

Dans cet article, on va **vous convaincre d'activer la MFA** avec un peu d'humour, beaucoup de bon sens, et surtout, sans mal de tête.

MFA, c'est quoi ? Un deuxième cadenas pour éviter la catastrophe

Le principe du **MFA (*Multi-Factor Authentication*)**, c'est simple :

Au lieu d'ouvrir un compte avec juste un mot de passe, on ajoute une couche de sécurité en plus.

Pourquoi ? Parce que les mots de passe, c'est fragile puisqu'ils sont faibles en général.

- Les gens utilisent **les mêmes mots de passe partout** (coucou "123456" utilisé sur *Facebook*, *Gmail* ET *Netflix*).
- Les hackers volent **des millions de mots de passe** chaque jour grâce aux fuites de données.
- Votre voisin de bureau qui vous espionne peut le voir taper (**on les connaît, ces fouineurs**).

Avec le **MFA**, même si un hacker met la main sur votre mot de passe, il lui faudra **une deuxième preuve** pour entrer. C'est comme si vous mettiez un digicode sur votre coffre-fort au lieu de laisser la clé sous le paillasson.

Les 3 types de MFA (et pourquoi vous en avez besoin)

Pour s'authentifier avec le MFA, il faut combiner **deux des trois facteurs suivants** :

Ce que vous savez (Facteur de connaissance)

✓ Un mot de passe (déjà compromis dans 90 % des cas).
✓ Un code PIN (un peu mieux, mais toujours vulnérable).

👉 **Problème** : Si quelqu'un le découvre, il peut l'utiliser.

Ce que vous possédez (Facteur de possession)

✓ Un code unique reçu par SMS ou une application d'authentification.
✓ Une clé de sécurité USB (pour les vrais pros).

👉 **Avantage** : Même si un hacker vole votre mot de passe, il n'a pas votre téléphone.

Ce que vous êtes (Facteur biométrique)

✓ Votre empreinte digitale.
✓ La reconnaissance faciale.
✓ Votre rétine (ok, là on commence à parler futuriste).

👉 **Avantage** : Impossible à deviner… sauf si vous avez un jumeau diabolique.

Comment activer la MFA et arrêter de vivre dangereusement

On ne va pas tourner autour du pot : **ACTIVEZ LA MFA SUR TOUS VOS COMPTES IMPORTANTS.**

📌 **Où l'activer ?**
✓ ***Gmail / Outlook / Yahoo*** (y a-t-il encore des gens qui utilisent *Yahoo* ? Pas certain…) parce qu'un pirate qui accède à vos mails peut réinitialiser tous vos comptes.
✓ ***Facebook***, ***Instagram***, **X** (imaginez un hacker postant un statut "J'adore les brocolis" à votre place).
✓ ***Amazon***, ***PayPal***, **banques** (vous tenez à votre argent, non ?).
✓ **Tout autre service qui propose la MFA** (quitte à être parano, autant le faire bien).

📌 **Comment l'activer ?**
Allez dans les paramètres de sécurité de votre compte.
Cherchez "Authentification à deux facteurs" (2FA) ou "MFA".
Choisissez votre méthode préférée :

- 📱 **Code par SMS** (**Mieux que rien, mais pas le plus sécurisé**).
- 🔑 **Appli d'authentification (*Google Authenticator, Microsoft Authenticator*)**.
- 🔐 **Clé de sécurité physique** (Pour les ultra-paranos).
  Suivez les instructions et ENJOY, votre compte est maintenant assez robuste 😊 !

« Mais c'est chiant de devoir valider à chaque fois ! »

Oui, et alors ? Vous voulez la sécurité **ou vous voulez pleurer parce que quelqu'un a pris le contrôle de votre compte *Facebook* et envoie des arnaques à tous vos contacts ?**

D'ailleurs, la plupart des services **se souviennent de vos appareils de confiance**. Résultat : vous n'aurez à entrer un code MFA que **si vous vous connectez depuis un nouvel appareil**.

Donc non, ce n'est pas si chiant. C'est juste **une habitude à prendre**, et croyez-moi, **c'est beaucoup moins « chiant » (désolé pour le terme…) que de se faire pirater**.

Les excuses « poches » pour ne pas activer la MFA (et pourquoi elles sont nulles)

🚫 **« J'ai rien à cacher. »**
👉 Cool, on va voir comment tu réagis quand un hacker poste "Mon boss est un crétin" sur ton compte *Facebook* et *Instagram*.

🚫 **« Ça n'arrive qu'aux autres. »**
👉 *LOL*, dites ça aux millions de victimes de fuites de données chaque année.

🚫 **« Je suis trop vieux pour ça. »**
👉 Ça prend 2 minutes à configurer, et promis, si vous savez envoyer un SMS, vous savez utiliser la MFA.

🚫 **« J'ai déjà un bon mot de passe. »**
👉 Et s'il fuit dans une base de données piratée ?

🚫 **« J'ai peur de perdre mon téléphone. »**
👉 Les applications d'authentification offrent **des sauvegardes et des options de récupération**. Vous n'aurez pas à paniquer.

Conclusion : Arrêtez de jouer avec le feu et activez la MFA !

Si vous tenez à vos comptes et à vos données personnelles, **il est temps d'arrêter de vivre dangereusement**.

🔥 **Un hacker avec votre mot de passe, c'est un hacker qui peut tout voler.**
🔥 **Un hacker qui rencontre la MFA, c'est un hacker frustré.**

Alors, plutôt que de regretter plus tard, **prenez 5 minutes pour activer la MFA sur vos comptes**. Votre futur vous remerciera (et évitera des sueurs froides).

👉 **Allez, foncez dans vos paramètres de sécurité et activez cette foutue MFA !** Vous me remercierez quand un hacker se cassera les dents en essayant d'accéder à votre compte. 😏
