Gestion des mots de passe : Une adoption lente, mais croissante des outils

Par Patrick Sentinel – 29a.ca

Statistiques sur l'utilisation des mots de passe : Un aperçu des pratiques actuelles

Les mots de passe demeurent l'une des principales méthodes d'authentification en ligne, malgré l'évolution des menaces et des pratiques en cybersécurité. Cependant, de nombreuses études révèlent que la majorité des utilisateurs continuent à adopter des pratiques à risque, compromettant la sécurité de leurs informations personnelles. Cet article propose un tour d'horizon des statistiques sur l'utilisation des mots de passe, révélant des tendances préoccupantes, mais aussi des pistes pour améliorer la cybersécurité.

Les mots de passe les plus courants : Une vulnérabilité courante

Les mots de passe les plus populaires demeurent extrêmement simples. Selon ***NordPass***, qui publie chaque année une liste des mots de passe les plus utilisés à partir de bases de données piratées, les résultats pour 2021 (oui, je suis d'accord… 2021 c'est un peu vieux) montrent que beaucoup d'utilisateurs continuent d'adopter des combinaisons trop faciles à deviner.

Rank	2021
1	123456
2	123456789
3	12345
4	qwerty
5	password
6	12345678
7	111111
8	123123
9	1234567890
10	1234567
11	qwerty123
12	000000
13	1q2w3e
14	aa12345678
15	abc123
16	password1
17	1234
18	qwertyuiop
19	123321
20	password123

[1]

[1] https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Les mots de passe de la liste précédente figurent souvent dans les premières tentatives des cybercriminels, en particulier lors d'attaques par force brute ou d'attaques par dictionnaire. Les statistiques montrent que ces mots de passe faibles peuvent être **craqués en moins d'une seconde 😬.**

Réutilisation des mots de passe : Une pratique à risque

Une autre statistique alarmante concerne la réutilisation des mots de passe. Selon une étude réalisée par ***Google* et *Harris Poll***, près de **52 %** des utilisateurs réutilisent le même mot de passe pour plusieurs comptes. Cela signifie que lorsqu'une fuite de données affecte un site, les autres comptes utilisant ce même mot de passe deviennent également vulnérables.

Pourquoi les utilisateurs réutilisent-ils leurs mots de passe?

- **Commodité** : Souvent, les utilisateurs trouvent plus simple de se souvenir d'un seul mot de passe, surtout lorsque chaque service en ligne exige des mots de passe différents. Ne succombez pas à la commodité et à la facilité 😊
- **Manque de sensibilisation** : de nombreux utilisateurs ne considèrent pas les risques associés à la réutilisation de mots de passe.

Longueur et complexité des mots de passe

Une étude de ***Spycloud*** réalisée en 2023 montre que plus de **30 %** des utilisateurs ont un mot de passe **de moins de huit caractères**, un chiffre préoccupant sachant que les recommandations en matière de sécurité préconisent des mots de passe **d'au moins 12 à 16 caractères** pour maximiser la robustesse.

- **17 %** des utilisateurs emploient des mots de passe comprenant uniquement des lettres;
- Moins de **30 %** des utilisateurs incluent des caractères spéciaux ou des chiffres dans leurs mots de passe.

Cette absence de complexité rend les mots de passe vulnérables aux attaques automatisées, qui testent rapidement des combinaisons simples.

Les gestionnaires de mots de passe sont considérés comme l'un des meilleurs moyens de renforcer la sécurité. Ils permettent de créer des mots de passe uniques et complexes sans avoir à les mémoriser. Cependant, leur adoption reste limitée.

D'après une enquête de ***Statista***, en 2022 :

- Seuls **25 %** des utilisateurs réguliers d'internet utilisent un gestionnaire de mots de passe;

- **45 %** des utilisateurs stockent encore leurs mots de passe sur des supports physiques ou numériques non sécurisés (45% c'est trop…), tels que des carnets ou des fichiers texte sur leur ordinateur.

Les gestionnaires de mots de passe

Parmi les raisons avancées pour expliquer la faible adoption des gestionnaires de mots de passe, on retrouve :

- **Méfiance envers ces outils** : Certains utilisateurs craignent que les gestionnaires eux-mêmes soient piratés.
- **Manque de compréhension** : De nombreux internautes ne comprennent pas le fonctionnement de ces outils ou leur utilité. Demandez de l'aide à une personne de confiance!

Authentification multifactorielle… Sous-utilisée

L'authentification multifactorielle (MFA), qui ajoute une couche de protection en demandant une preuve d'identité supplémentaire (souvent un code envoyé sur un téléphone), est une pratique recommandée par la majorité des experts en sécurité. Cependant, selon un rapport de ***Microsoft***, seulement **11 %** des utilisateurs l'activent lorsqu'elle est proposée, malgré le fait que cela réduise considérablement le risque de piratage.

Pourquoi la MFA est-elle si peu adoptée?

- **Complexité perçue** : Beaucoup d'utilisateurs considèrent que la MFA rend l'accès à leurs comptes plus difficile ou fastidieux.
- **Ignorance des risques** : Il existe une méconnaissance des bénéfices de la MFA, avec de nombreux utilisateurs pensant que leur mot de passe est suffisant pour protéger leurs comptes.

Conséquences des mauvaises pratiques : Les fuites de données en hausse

Les statistiques démontrent que des pratiques faibles en matière de mots de passe ont des conséquences directes sur les cyberattaques. En 2022, selon la ***Verizon Data Breach Investigations Report*** :

- **81 %** des violations de données ont été causées par des mots de passe volés ou faibles.
- Les cyberattaques par vol d'identifiants continuent de croître à un rythme inquiétant.

Ces chiffres montrent que l'utilisation généralisée de mots de passe faibles ou réutilisés amplifie les risques de cyberattaques pour les entreprises et les particuliers.

Conclusion

Les statistiques sur l'utilisation des mots de passe révèlent des tendances préoccupantes! Des mots de passe trop simples, une réutilisation excessive, et une adoption limitée des outils et pratiques qui renforcent la sécurité. Face à ces défis, il devient essentiel de promouvoir de meilleures pratiques, telles que l'adoption de gestionnaires de mots de passe, l'activation de l'authentification multifactorielle, et la création de mots de passe plus longs et plus complexes. Ces mesures permettront de réduire les risques liés aux mots de passe faibles et de protéger les utilisateurs des cybermenaces.