

AUTHENTIFICATION MULTIFACTORIELLE

Nos appareils et comptes sont des outils importants qui nous relient au monde. Mais nous y stockons beaucoup de renseignements personnels et nous ne voulons surtout pas que ces renseignements tombent entre les mains de criminels. Dès lors, comment pouvons-nous faire en sorte que ces renseignements demeurent confidentiels ? En utilisant non seulement des mots de passe robustes, mais aussi en activant l'authentification multifactorielle, qui exige un deuxième facteur d'identification pour pouvoir accéder à nos appareils et comptes.

L'AUTHENTIFICATION MULTIFACTORIELLE : SUR MESURE POUR VOUS

QUI VOUS ÊTES

- Lecteurs d'empreintes digitales
- Appareils de reconnaissance vocale
- Appareils de reconnaissance faciale

CE QUE VOUS SAVEZ

- Questions de sécurité
- Mots et phrases de passe
- NIP

CE QUE VOUS POSSÉDEZ

- Authentification par message texte
- Authentification par application
- Jetons informatiques



LE SAVIEZ-VOUS ?

1 sur 3 : proportion de Canadiens qui utilisent l'authentification multifactorielle¹

Une simple authentification en deux étapes vous protège contre :

- 100 % des robots automatisés
- 96 % des attaques par hameçonnage
- 76 % des attaques ciblées²

81 % des vols de données par piratage sont dues à des mots de passe faibles ou volés³

L'AUTHENTIFICATION MULTIFACTORIELLE PEUT VOUS PROTÉGER

Activer l'authentification multifactorielle peut vous aider à protéger vos renseignements personnels contre les cybercriminels.

Certains outils d'authentification, comme ceux par message texte ou applications, peuvent vous prévenir que vous êtes victime d'une attaque pour accéder à vos comptes.

¹ Santé publique Canada, Sondage auprès des utilisateurs d'Internet au sujet de la cybersécurité, EKOS Research Associates, 2018

² New research: How effective is basic account hygiene at preventing hijacking, Google Security Blog, 2019

³ 2017 Data Breach Investigations Report, Verizon, 2017