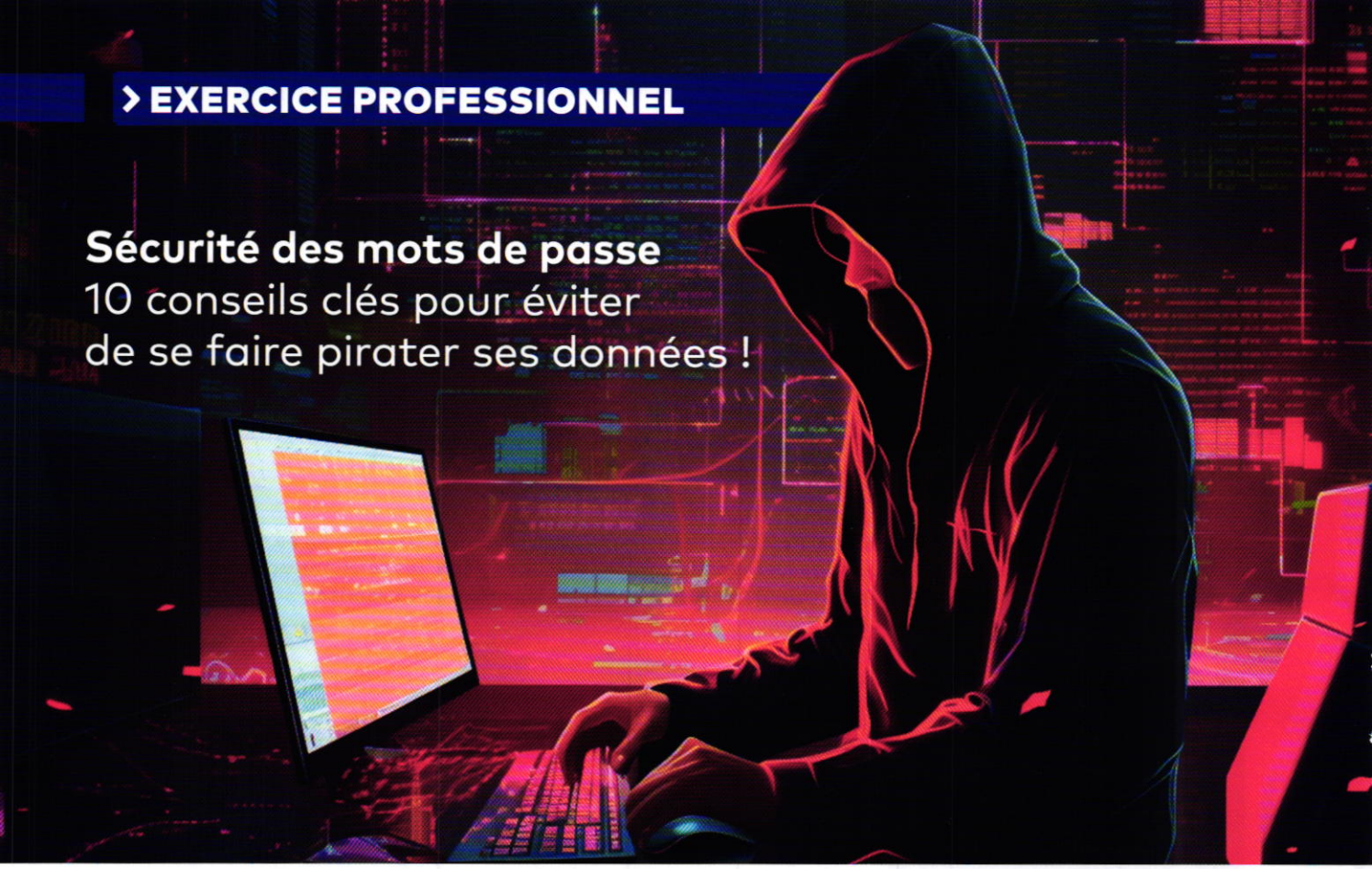
Sécurité des mots de passe
10 conseils clés pour éviter de se faire pirater ses données !



PAR **CONSTANCE CAMILLERI**,
DIRECTRICE PROSPECTIVE
ET PERFORMANCE,
CONSEIL NATIONAL

Le 7 mai, c'était la journée mondiale du mot de passe. L'occasion de renforcer la sécurité de ceux que vous utilisez et de prendre des mesures pour protéger véritablement vos données. Voici 10 conseils clés de sécurité faisant le plus souvent appel à du simple bon sens pour se prémunir des attaques.

On sait que le mot de passe le plus utilisé en 2022 est le même depuis 2011 : «123456 », autrement dit le niveau zéro de la sécurité... Et sans aucun doute le premier mot de passe auquel songent les cybercriminels, par le biais d'un logiciel qui teste un à un les codes les plus utilisés en une fraction de seconde. On comprend tout de suite mieux pourquoi il est si simple de deviner un mot de passe...

LE SAVIEZ-VOUS ?

2 secondes seulement suffisent pour casser un mot de passe de 12 caractères uniquement composé de chiffres ! Le tableau ci-après présente un récapitulatif assez parlant du temps qu'il faudrait à un cybercriminel pour hacker un mot de passe en fonction des caractères employés (longueur, chiffres, lettres, symboles, mélange...). Cela confirme l'importance de disposer de mots de passe robustes en tenant compte à la fois de leur longueur, mais aussi de leur complexité.

Pour sécuriser vos données, il est donc indispensable de choisir avec soin des mots de passe robustes et complexes à deviner. N'oubliez pas que vous participez à la protection des informations du cabinet en étant responsables des droits et codes que vous pourriez donner (ou laisser facilement découvrir...) à d'autres utilisateurs.