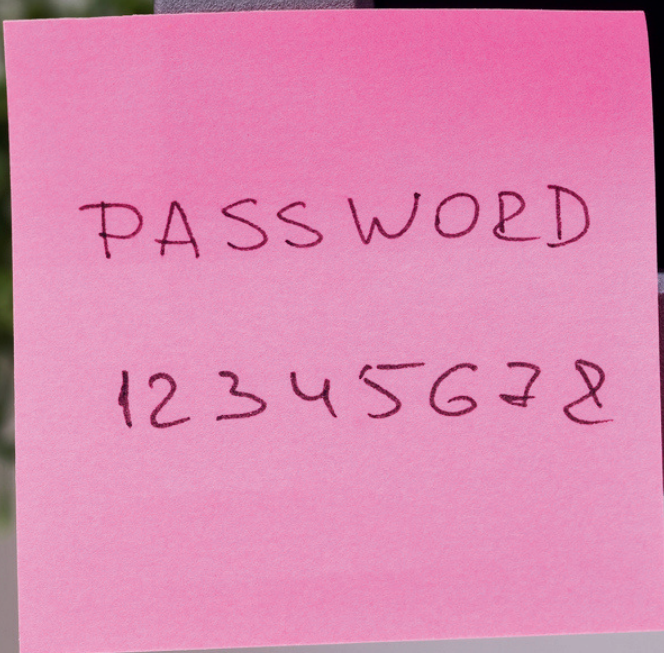
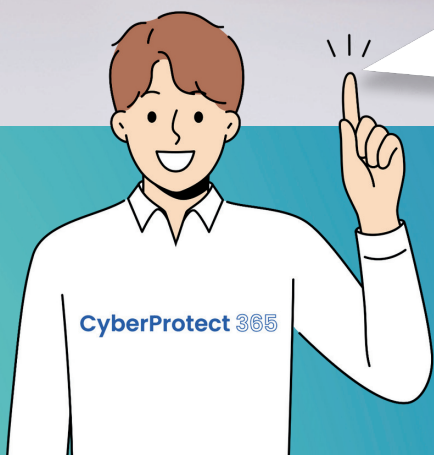


Les hackers vous disent merci

80% des violations de données sont liées à des mots de passe faibles ou compromis.



PASSWORD
12345678



Protégez vos données, choisissez des mots de passe complexes et sauvegardez-les sur des plateformes sécurisées.

Le mot de passe le plus courant est « 123456 », ce qui prendrait moins d'une seconde aux pirates pour le craquer.

« Mot de passe » est le terme le plus couramment utilisé par les pirates pour accéder aux réseaux d'entreprise.

45 % des personnes interrogées n'ont pas changé leurs mots de passe au cours de l'année écoulée, même après une violation.

36% des personnes estiment (à tort !) que leurs comptes ne sont pas suffisamment précieux pour les pirates.

Hum... LinkedIn ou LinkedIn ?

3,4 milliards d'e-mails de phishing sont envoyés chaque jour, soit plus de 1 000 milliards par an.

LinkedIn

Bonjour Alexandre,

Vous avez ajouté une nouvelle adresse e-mail à votre compte LinkedIn.

Pour confirmer cette adresse veuillez cliquer sur [ce lien](#) ou le coller dans votre navigateur :

<https://www.linkedin.com/psettings/sign-in-and-security>

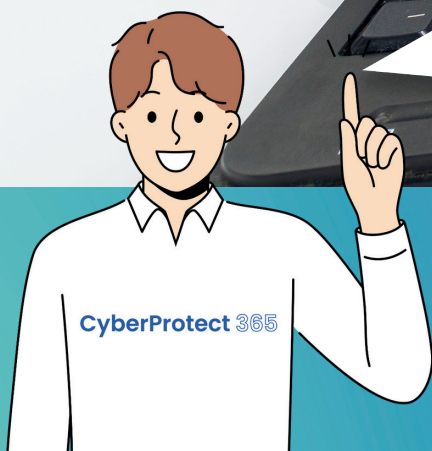
Nous vous demanderons ensuite de vous identifier. Assurez-vous d'utiliser l'adresse e-mail sur laquelle vous souhaitez recevoir les messages, les invitations et les demandes.

Merci d'utiliser LinkedIn !
L'équipe LinkedIn

[Se désinscrire](#) | [Aidez-moi](#)



Vérifiez bien l'adresse de l'expéditeur, et préférez toujours passer par les sites officiels plutôt que de cliquer sur les liens.



En 2024, 89 % des e-mails de phishing impliquaient des tactiques d'usurpation d'identité, Adobe étant la marque la plus usurpée (LinkedIn en 2022).

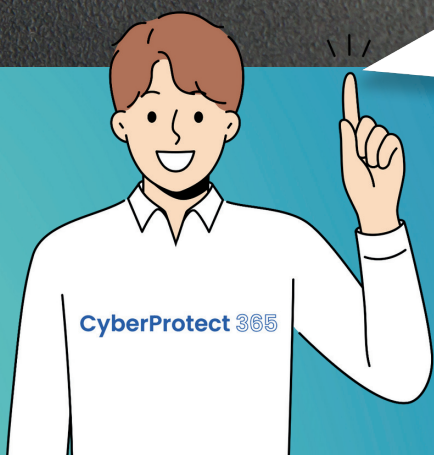
Les cybercriminels se tournent de plus en plus vers les comptes professionnels entraînant 2,8 milliards d'euro de pertes par an.

30 % des petites entreprises considèrent le phishing comme leur principale menace en matière de cybersécurité.

En 2024, 67,4 % des attaques de phishing ont utilisé l'intelligence artificielle pour créer des contenus plus convaincants.

Si seulement c'était aussi évident...

45 % des personnes qui trouvent une clé USB la branchent sur leur ordinateur.



Si vous trouvez une clé USB, remettez-la au service informatique ou au centre des opérations de sécurité compétent, sans tenter de consulter son contenu.

En 2024, 51 % des attaques de malware étaient conçues pour cibler des dispositifs USB.

90 % des employés utilisent des clés USB, et parmi eux, 80 % utilisent des clés non chiffrées.

Les clés USB de piratage, appelées « Rubber Duckies », peuvent simuler l'action d'un clavier et générer des frappes prédéfinies à une vitesse de plus de 1 000 mots par minute, permettant ainsi aux attaquants d'installer des portes dérobées, de voler des documents ou des mots de passe, ou encore d'établir des droits étendus sur l'ordinateur ciblé.