LES BONS RÉFLEXES FACE AUX CYBERATTAQUES

Face aux cyberattaques, de plus en plus fréquentes, voici quelques conseils du GroupeFBO !

GROUPEFBO

POURQUOI EST-IL IMPORTANT DE RESTER VIGILANT ?

Aujourd'hui, les cyberattaques sont de plus en plus nombreuses et paralysent beaucoup d'entreprises durant plusieurs jours, semaines, voire des mois avec des pertes considérables.

Au-delà de la mise en place des systèmes informatiques performants, modernes et sécurisés, un autre point doit attirer votre attention : celui du comportement humain sur les postes de votre entreprise.

"

Vous, utilisateur, êtes la première barrière pour lutter contre les cyberattaques. Il est donc primordial que vous soyez attentifs à ce que vous faites sur vos postes (mails, sites consultés, téléchargements...).

Nous pouvons installer les systèmes informatiques les plus modernes et efficaces, si vous compromettez votre mot de passe ou votre navigateur par un clic malencontreux, nous ne pourrons protéger votre système informatique de cette inattention.

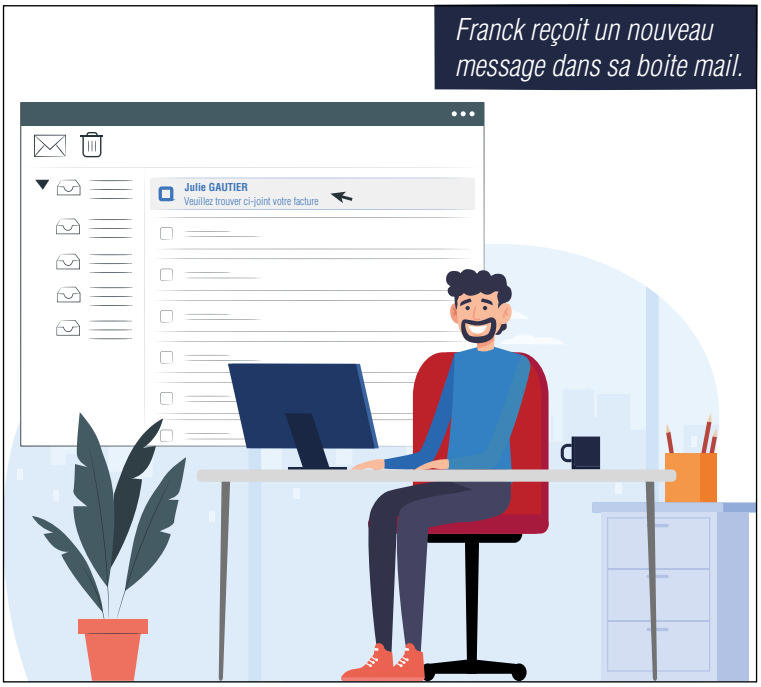
Pour vous aider à rester vigilant, nous vous donnons quelques conseils que vous devez appliquer au quotidien.

Dominique
Responsable Systèmes & Réseaux

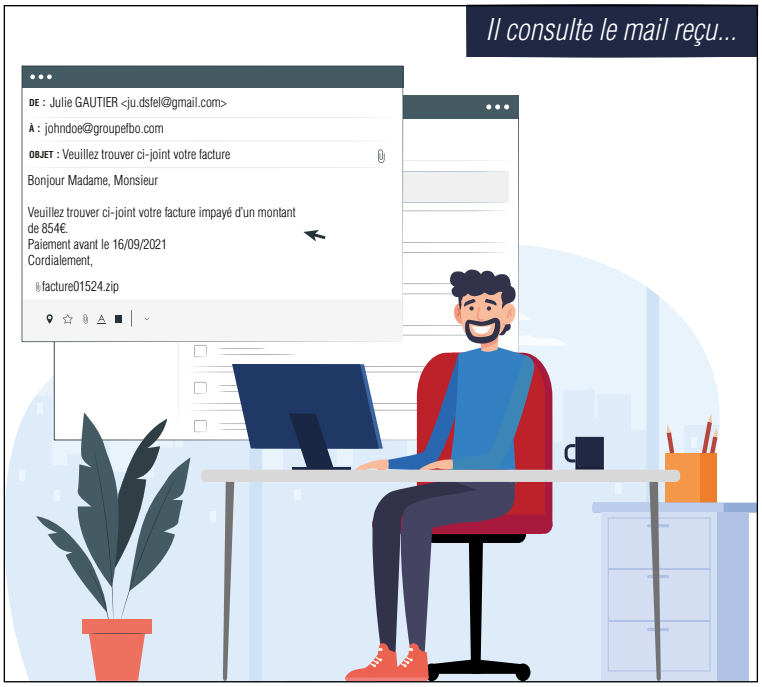
Voici quelques bonnes pratiques

1. Soyez vigilant sur les mails que vous recevez

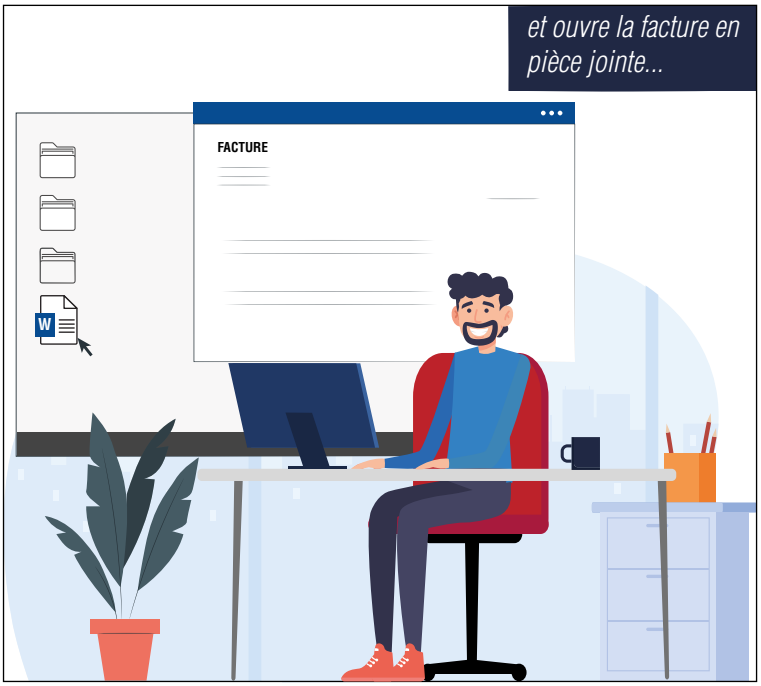
Franck reçoit un nouveau message dans sa boite mail.



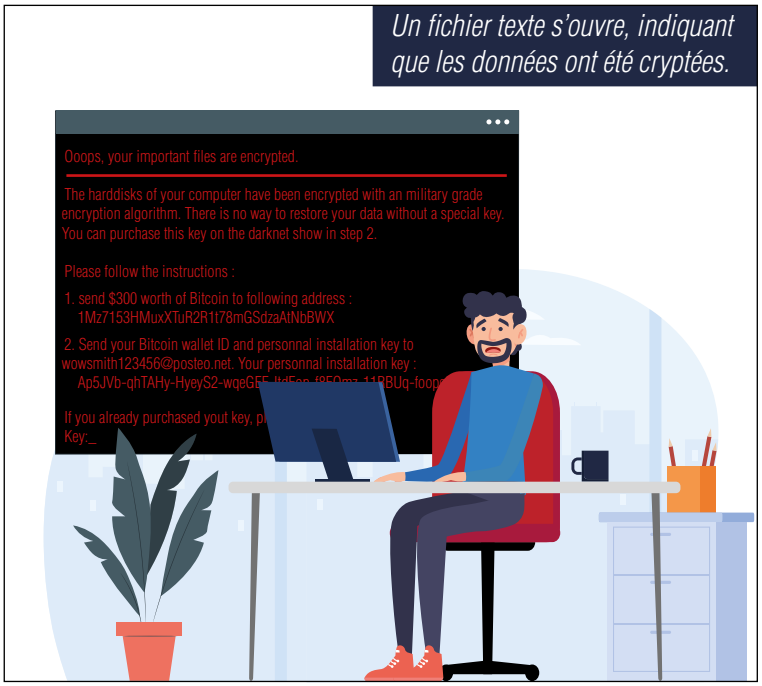
Il consulte le mail reçu...



et ouvre la facture en pièce jointe...



Un fichier texte s'ouvre, indiquant que les données ont été cryptées.



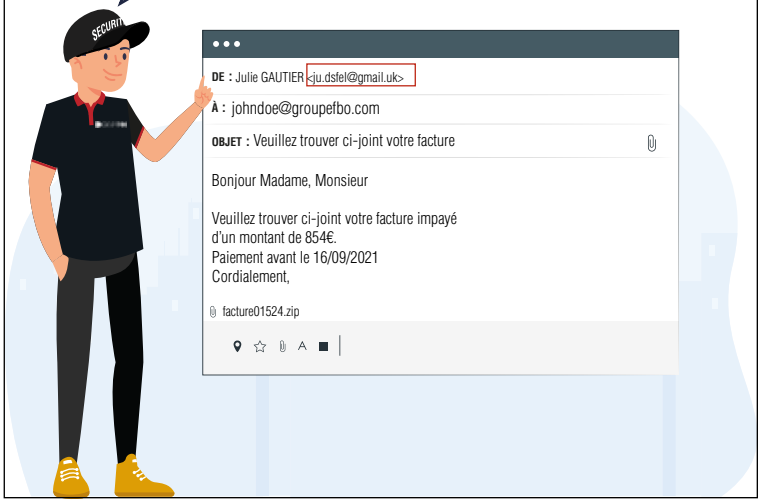
Les conseils GroupeFBO

Le hameçonnage (consistant à inciter le destinataire à cliquer sur un lien ou une pièce jointe) est une méthode très répandue. Il est important, que vous, utilisateur, soyez vigilant au mail que vous recevez pour ne pas tomber dans le piège.

Bien souvent, ces mails sont très proches de la réalité, cependant quelques points peuvent vous alerter.

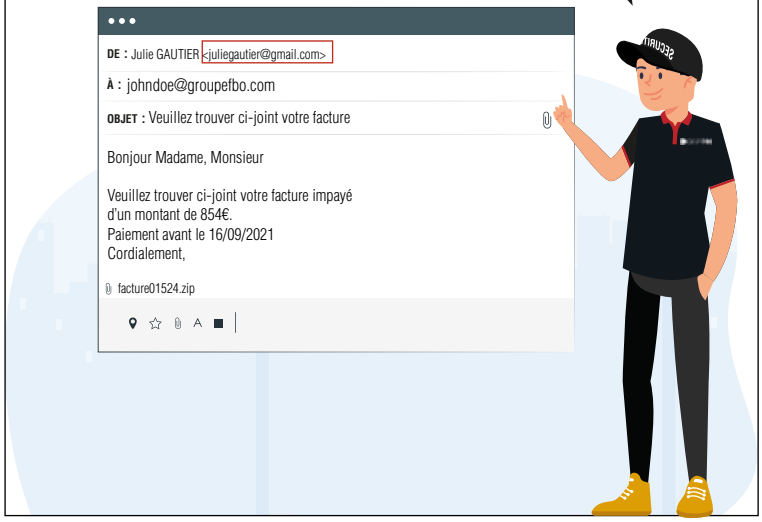
1. L'adresse e-mail de l'expéditeur

Si celle-ci vous est inconnue ou que le mail vous semble suspect, vérifiez l'adresse mail entre les chevrons.



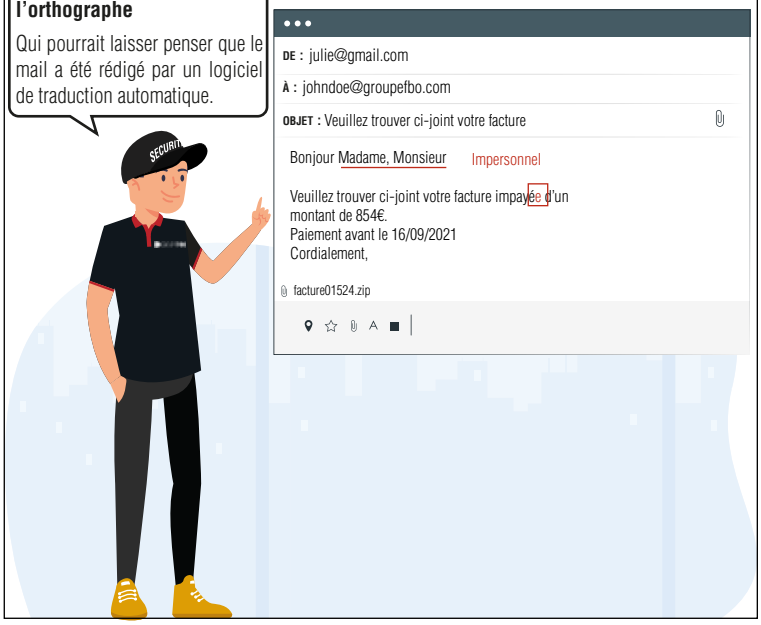
2. La pertinence du message

Même si l'adresse mail vous semble viable, vérifiez la cohérence entre l'expéditeur et le contenu du mail. En cas de doute, contactez directement l'émetteur du mail.



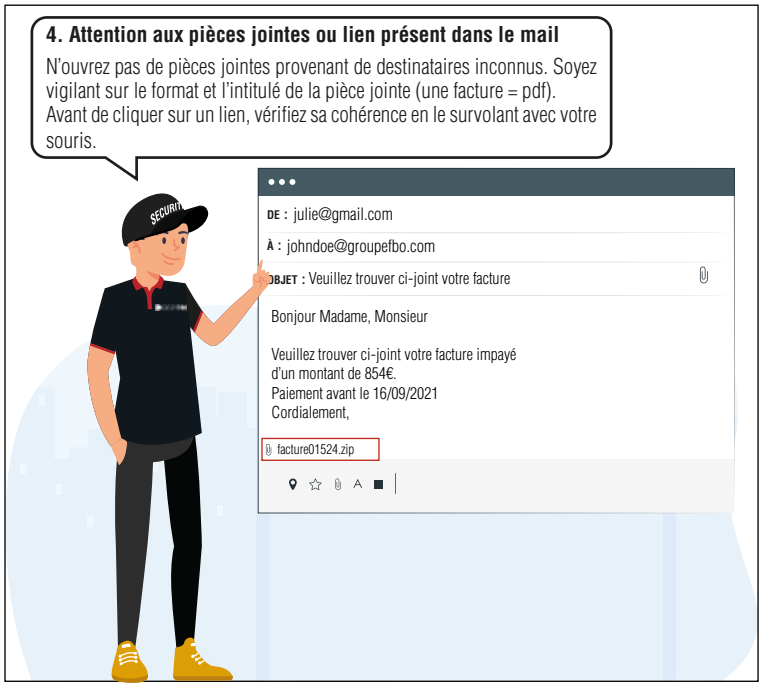
3. La syntaxe et l'orthographe

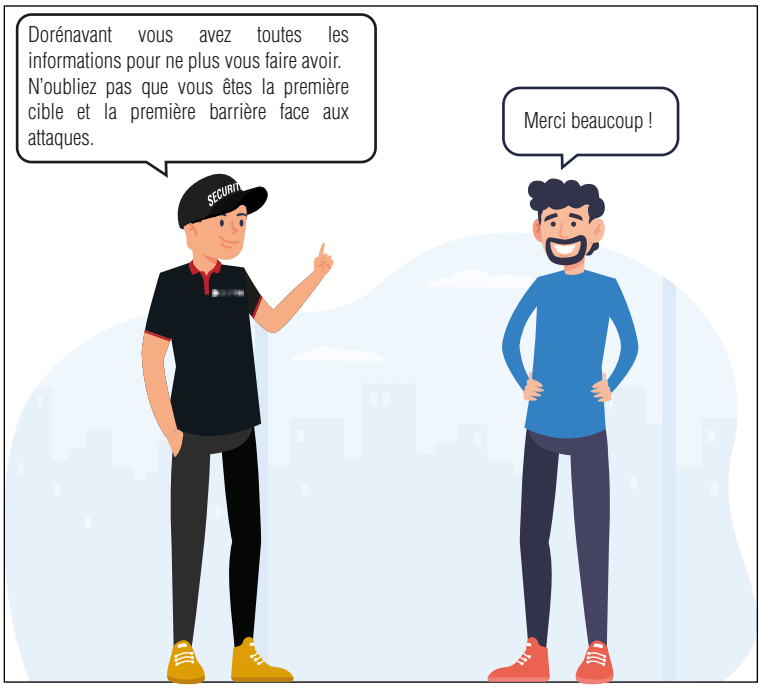
Qui pourrait laisser penser que le mail a été rédigé par un logiciel de traduction automatique.



4. Attention aux pièces jointes ou lien présent dans le mail

N'ouvrez pas de pièces jointes provenant de destinataires inconnus. Soyez vigilant sur le format et l'intitulé de la pièce jointe (une facture = pdf). Avant de cliquer sur un lien, vérifiez sa cohérence en le survolant avec votre souris.





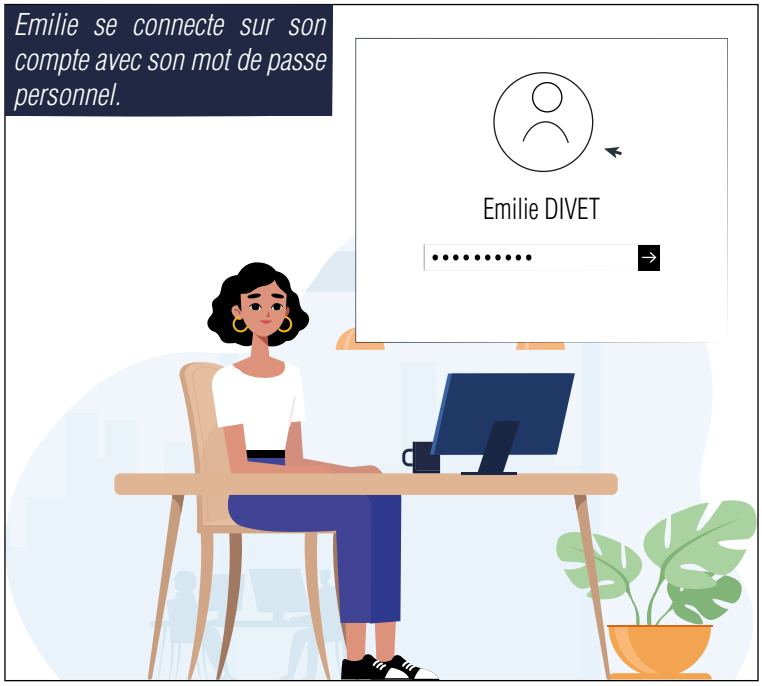
Les conseils GroupeFBO

- Ne communiquez jamais de données confidentielles en réponse à un mail (code, numéro de carte bancaire...)
- N'appelez jamais de numéro que vous ne connaissez pas provenant d'un mail.

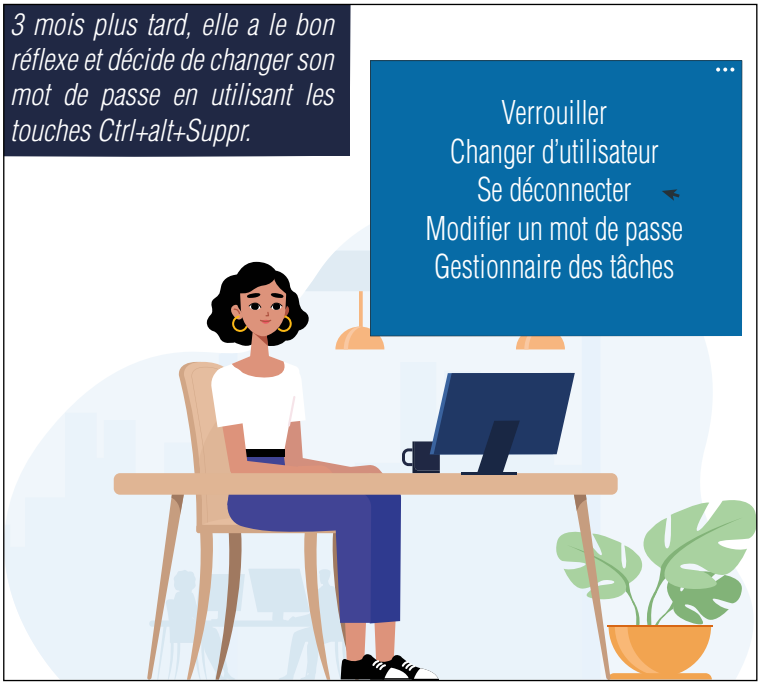
Au moindre doute, renseignez vous avant de cliquer.

2. Les mots de passe

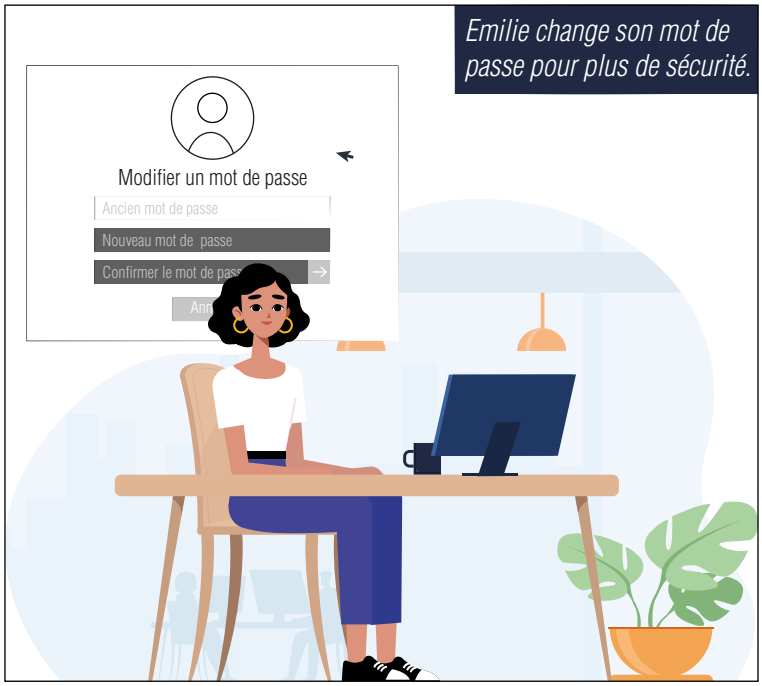
Emilie se connecte sur son compte avec son mot de passe personnel.



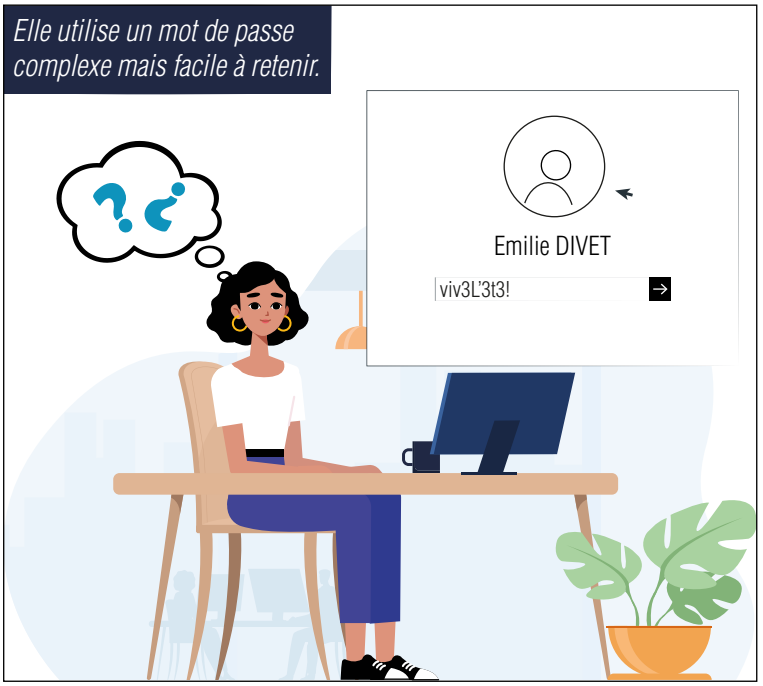
3 mois plus tard, elle a le bon réflexe et décide de changer son mot de passe en utilisant les touches Ctrl+alt+Suppr.



Emilie change son mot de passe pour plus de sécurité.



Elle utilise un mot de passe complexe mais facile à retenir.



Les conseils GroupeFBO

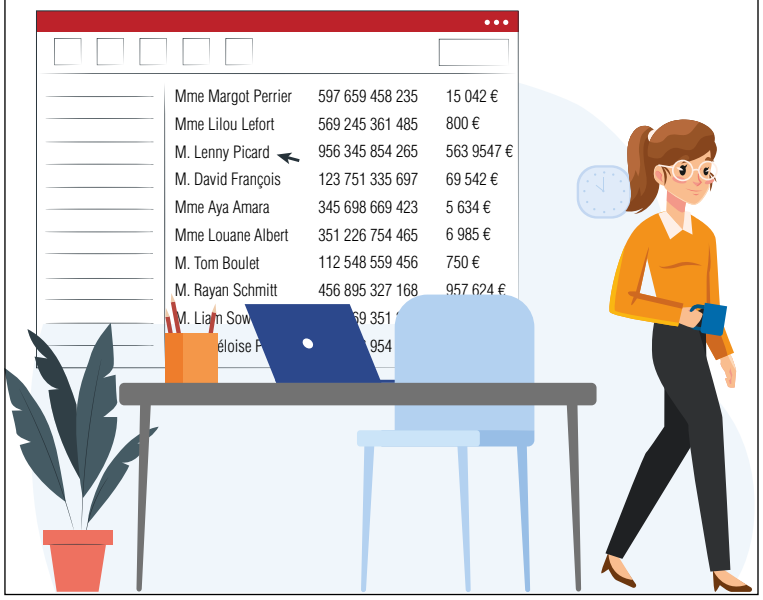
- Utilisez des mots de passe différents pour vos comptes personnels et professionnels.
- Ne notez pas vos mots de passe sur votre bureau.
- Ne divulguez pas vos mots de passe à quiconque.
- Utilisez des lettres, des chiffres, des caractères spéciaux, des majuscules et minuscules. (min 10 caractères)

Pour retenir facilement vos mots de passe utilisez une phrase «jeSuisaut0pdel@s3curit3e!»

3. Verrouillage de son poste de travail

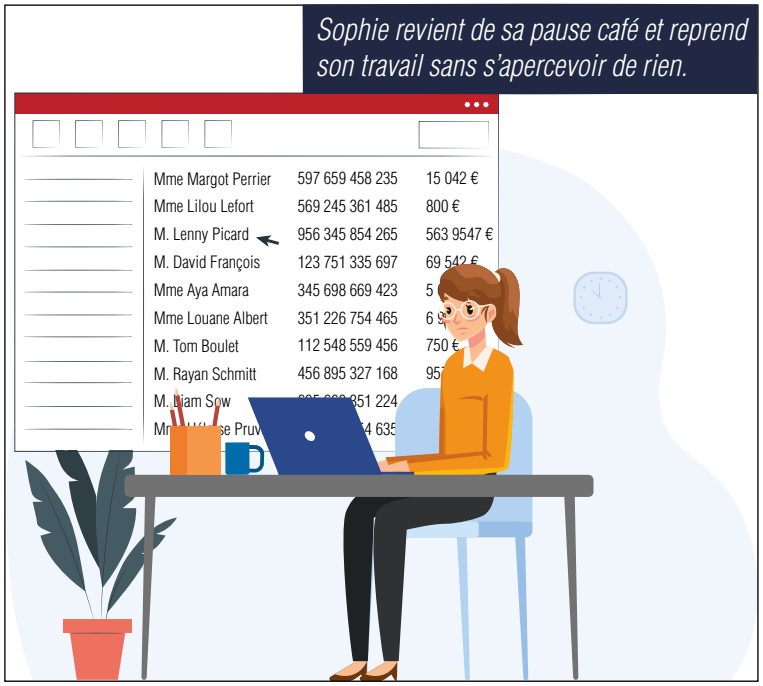
Sophie travaille sur la gestion commerciale de l'entreprise .

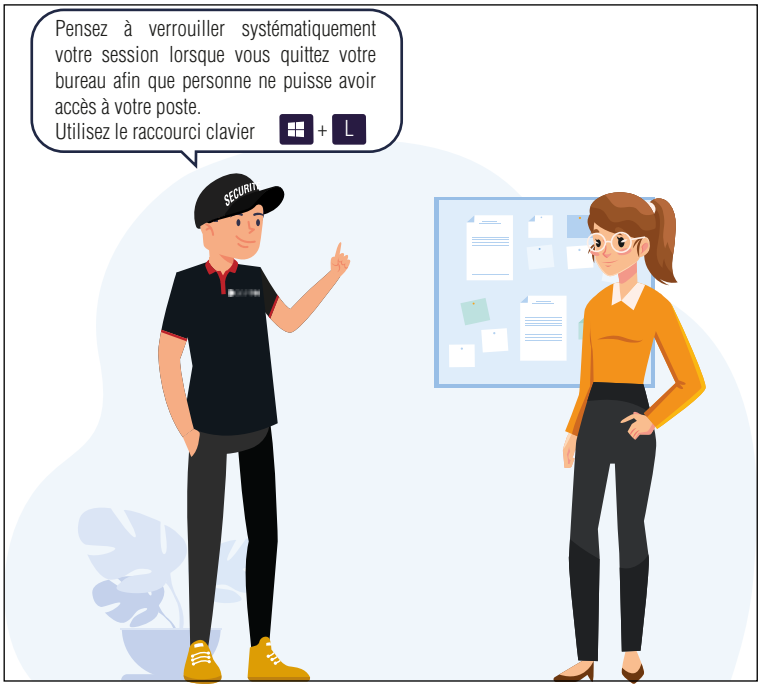
Elle part prendre un café en laissant sa session ouverte.



Une personne s'introduit à son poste pour télécharger les données clients.

Sophie revient de sa pause café et reprend son travail sans s'apercevoir de rien.



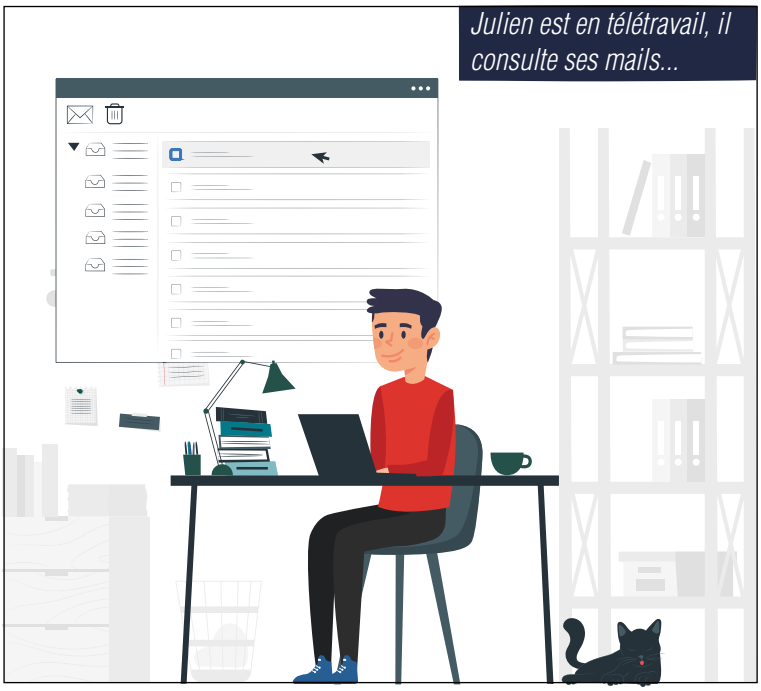


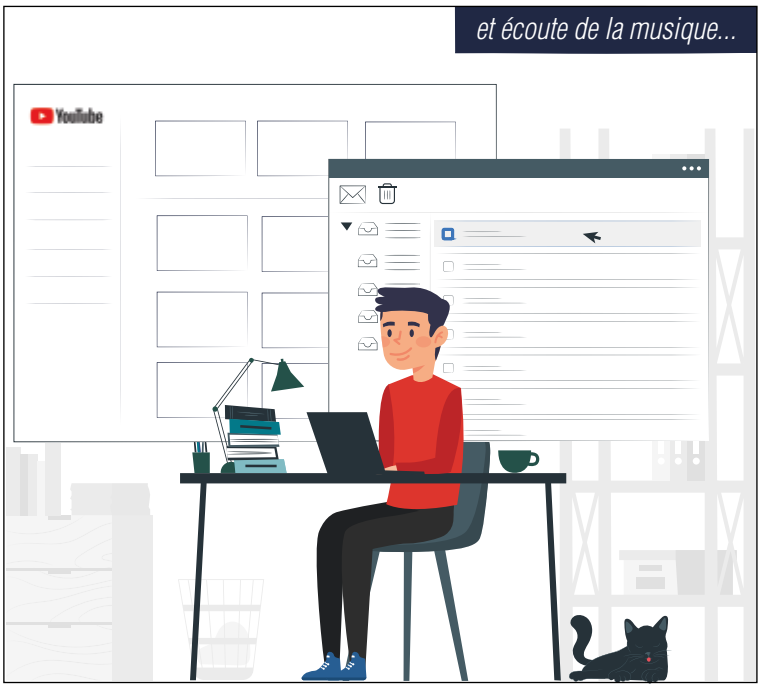
Les conseils GroupeFBO

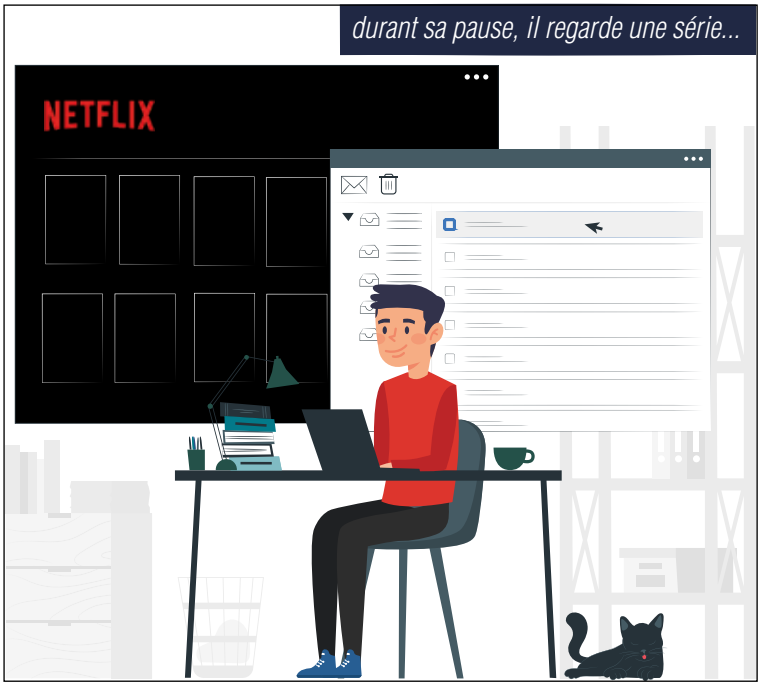
- Pensez à verrouiller votre ordinateur lorsque vous quittez votre bureau, n'importe qui pourrait utiliser votre identité et envoyer des mails à votre insu.
- Soyez vigilant sur les personnes qui interviennent sur votre poste et assurez vous de leur identité pour éviter tout problème.
- Ne donnez pas la main sur votre ordinateur à n'importe qui.

En cas de doute, n'hésitez pas à nous contacter !

4. Utilisation du VPN en télétravail







Les conseils GroupeFBO

En télétravail, l'utilisation de votre ordinateur doit rester dans le cadre professionnel pour limiter les risques de piratage.

- Soyez vigilant sur les sites que vous consultez (site sécurisé).
- Attention à l'utilisation de clé USB personnelle.

En cas de doute référez-vous systématiquement à votre service informatique et surtout ne contactez pas un numéro de téléphone inconnu.

QUELQUES CONSEILS SUPPLÉMENTAIRES

- Ne branchez jamais sur votre poste une clé USB que vous avez trouvé et dont vous ne connaissez ni le contenu, ni le propriétaire.

- Lorsque vous recevez une mail frauduleux, bien souvent, tout vous semblera normal mais prenez du recul sur la pertinence des messages par rapport à l'expéditeur. N'importe qui peut être victime d'usurpation, même les plus grands organismes (impôt, banque, CPF...). Un moyen de communication différents doit vous alerter.

ET SI VOUS CLIQUEZ SUR UN LIEN MALENCONTREUSEMENT...

- Si on vous recommande d'appeler un numéro de téléphone pour débloquer votre PC, surtout, ne le faites pas et contactez votre service informatique.

- Ne communiquez jamais d'informations personnelles, ni de coordonnées bancaires par téléphone, mail ou SMS.

GroupeFBO
02 51 34 24 66