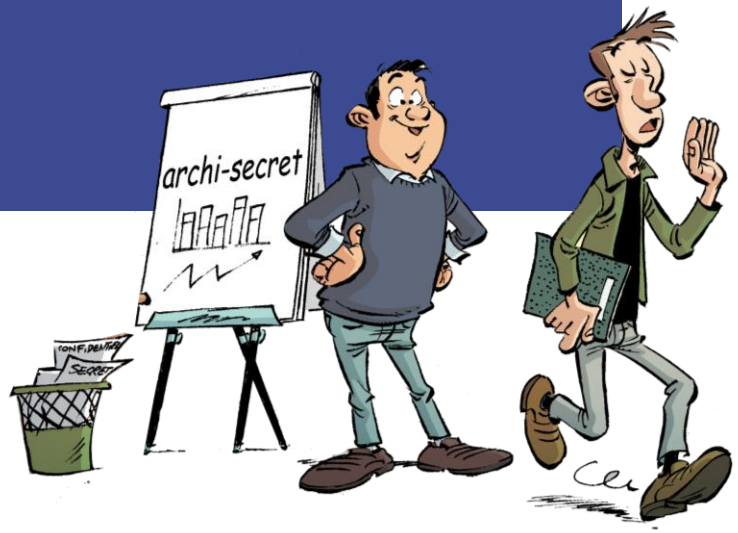
BONNES PRATIQUES

À DESTINATION DE L'ENSEMBLE DES COLLABORATEURS

SENSIBILISATION À LA SÉCURITÉ DU SYSTÈME D'INFORMATION

GROUPE PASTEUR MUTUALITÉ



www.corporatefiction.fr – Mai 2022 – Illustrations : Léturgie

SENSIBILISATION À LA SÉCURITÉ
DU SYSTÈME D'INFORMATION

Le RÔLE ESSENTIEL des collaborateurs

GROUPE PASTEUR MUTUALITÉ

www.corporatefiction.fr – Mai 2022 – Illustrations : Léturgie

SENSIBILISATION À LA SÉCURITÉ DU SYSTÈME D'INFORMATION

1. Quel est le contexte ?
2. La sécurité est l'affaire de tous.
3. Les principes fondamentaux à adopter.
4. En savoir plus sur les recommandations à suivre.

GROUPE PASTEUR MUTUALITÉ

www.corporatefiction.fr – Mai 2022 – Illustrations : Léturgie

DES CYBERMENACES EN RECRUDESCENCE

Les entreprises sont de plus en plus menacées…

Baromètre des risques 2020 : la cybersécurité devient **la 1ère préoccupation des entreprises.**

Recrudescence des cyberattaques, sans distinction du secteur d'activité ou de la taille.

par des attaques qui peuvent avoir de lourdes conséquences.

Impact financier significatif et forte médiatisation (risque de conformité, d'image et de notoriété).

Arrêt de la production, indisponibilité des systèmes : retour au papier et crayon.

GROUPE PASTEUR MUTUALITÉ

QUELQUES EXEMPLES DE CYBERATTAQUES

Ramsay Santé

Le 15 août 2019, **Ramsay Santé** est victime d'une grande cyberattaque qui se propage au sein de 120 établissements en France, avec comme résultat le chiffrement des données.

BOUYGUES CONSTRUCTION

En janvier 2020, le géant du **BTP Bouygues Construction** a été touché par une vaste cyberattaque, avec à la clé : la divulgation, le chiffrement des données.

MNH

En février 2021, la **Mutuelle nationale des hospitaliers (MNH)** reprend ses activités, plusieurs semaines après avoir été victime d'une cyberattaque par chiffrement des données.

Point commun

Une demande de rançon est formulée lors de ces différentes attaques

GROUPE PASTEUR MUTUALITÉ

TOUS EXPOSÉS AU PHISHING

80% **des attaques informatiques impliquent la technique d'hameçonnage (phishing)**

La grande majorité de ce type d'attaque est opérée et facilitée par l'hameçonnage profitant de la négligence des utilisateurs. Ces lacunes peuvent être comblées par des gestes simples et de bonnes habitudes.

À RETENIR

CHAQUE COLLABORATEUR A UN RÔLE À JOUER DANS LA CHAÎNE DE DÉTECTION ET DE PROTECTION DES DONNÉES DE L'ENTREPRISE.

GROUPE PASTEUR MUTUALITÉ

SENSIBILISATION À LA SÉCURITÉ DU SYSTÈME D'INFORMATION

1. Quel est le contexte ?
2. La sécurité est l'affaire de tous.
3. Les principes fondamentaux à adopter.
4. En savoir plus sur les recommandations à suivre.

GROUPE PASTEUR MUTUALITÉ

www.corporatefiction.fr – Mai 2022 – Illustrations : Léturgie

LA SÉCURITÉ EST L'AFFAIRE DE TOUS

Un sujet porté par les membres de l'Office Sécurité du Système d'Information

« Face aux risques croissants liés à la cybersécurité et à la sensibilité des données que nous manipulons au sein de Groupe Pasteur Mutualité, chaque collaborateur est un acteur de la sécurité de l'information au quotidien. »

Message du Directeur Général
de Groupe Pasteur Mutualité

« Pour vous accompagner, un plan de sensibilisation à la sécurité du système d'information, est à votre disposition, ce qui vous permettra de détecter au mieux les menaces et d'éviter les attaques de grande ampleur. »

Message du RSSI
de Groupe Pasteur Mutualité

GROUPE
PASTEUR
MUTUALITÉ

SENSIBILISATION À LA SÉCURITÉ DU SYSTÈME D'INFORMATION

1. Quel est le contexte ?
2. La sécurité est l'affaire de tous.
3. Les principes fondamentaux à adopter.
4. En savoir plus sur les recommandations à suivre.

GROUPE PASTEUR MUTUALITÉ

www.corporatefiction.fr – Mai 2022 – Illustrations : Léturgie

LES BONNES PRATIQUES

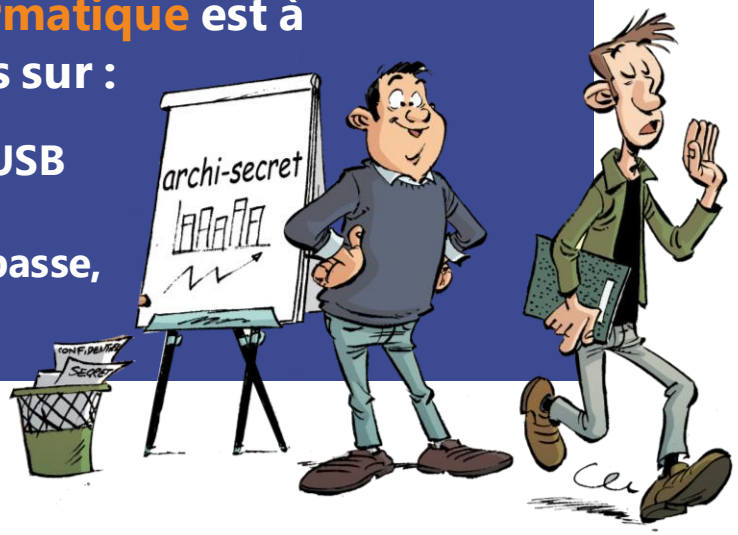
3 principes fondamentaux à adopter par l'ensemble des collaborateurs de Groupe Pasteur Mutualité :

1. Choisir avec soin ses mots de passe
2. Séparer les usages personnels et professionnels
3. Prendre soin de ses informations

EN SAVOIR +

Pour aller plus loin, votre service informatique est à vos côtés pour vous en apprendre plus sur :

- la navigation internet, le cloud, les clés USB
- les déplacements, l'ingénierie sociale
- la confidentialité du mot de passe, les nouveaux modes d'authentification



GROUPE PASTEUR MUTUALITÉ

MOT DE PASSE ROBUSTE

Quels **risques** en cas de négligence ?

- Usurpation d'identité,
- Accès facilité aux informations sensibles et aux données de l'entreprise (messagerie, espace OneDrive, applications, ...).

Le saviez-vous ? :

Le temps nécessaire pour deviner un mot de passe :

- Charlotte : 3 secondes
- Ch@rlotte@les2yeuxbleus : 8477 siècles

LES BONNES PRATIQUES :

- Je crée des **mots de passe robustes,** longs avec au moins 12 caractères et complexes, de préférence une phrase.
- **J'adopte l'authentification renforcée** pour mes accès en mobilité (utilisation de l'application mobile **Microsoft Authenticator**).

GROUPE PASTEUR MUTUALITÉ

HAMEÇONNAGE

Quels **risques** en cas de négligence ?

- Fraude,
- Indisponibilité du système d'information faisant suite à la propagation de codes malveillants,
- Divulgation de données (données d'entreprise, des adhérents, des partenaires, …).

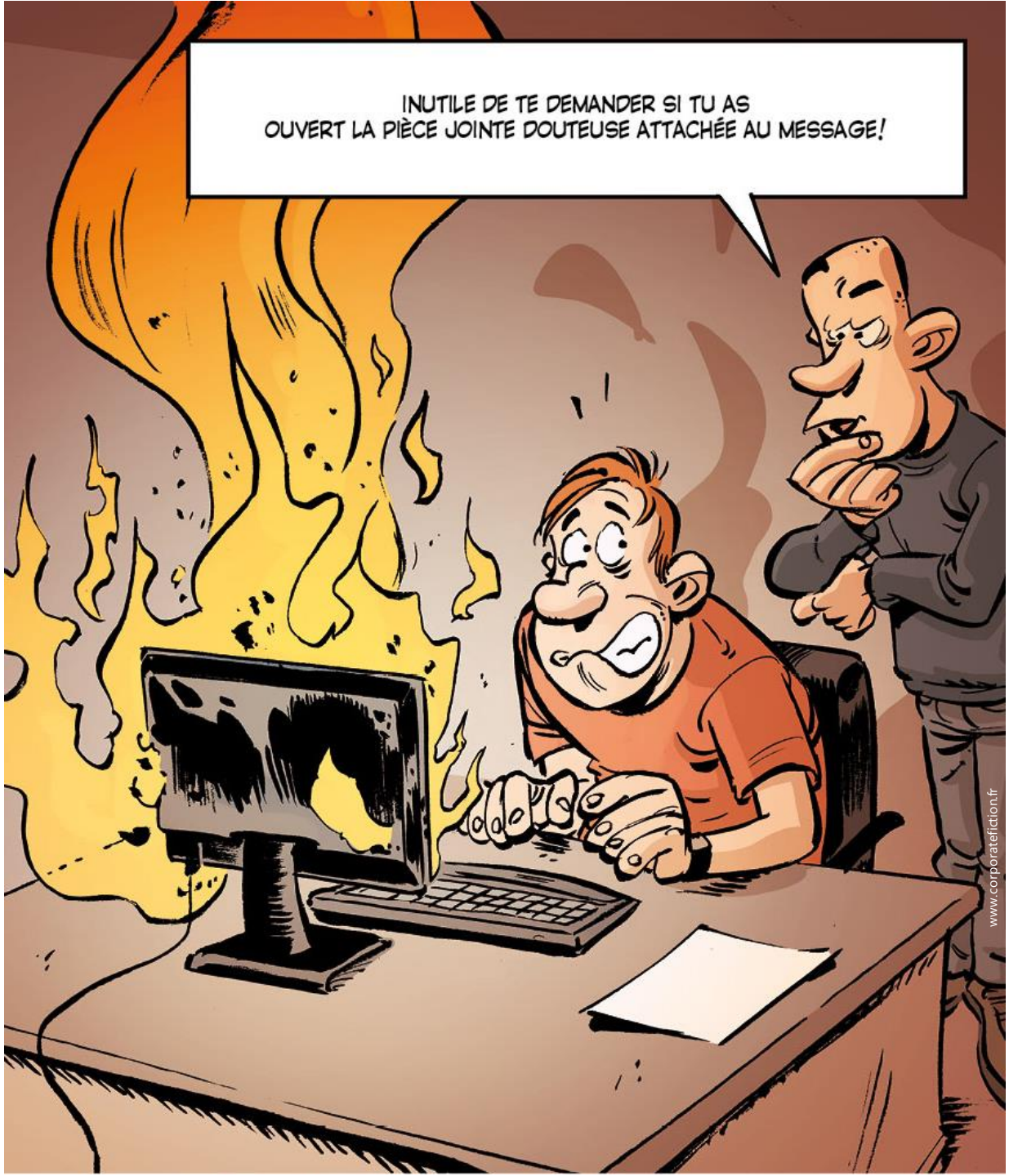
Action rapide :

- Signaler tout courriel suspect ou malveillant à l'aide de la fonctionnalité « **Report phishing** » depuis votre client de messagerie Outlook.

LES BONNES PRATIQUES :

- Je vérifie la **vraisemblance du message.**
- **Je survole sans cliquer les liens et adresses** d'expéditeurs pour en vérifier la légitimité.
- Au moindre doute ou anomalie sur mon poste de travail, **je contacte le support informatique.**

GROUPE PASTEUR MUTUALITÉ



SÉPARATION DES USAGES

Quels **risques** en cas de négligence ?

- Fuite, perte de données,
- Indisponibilité des données faisant suite à la contamination du système d'information.

Constat :

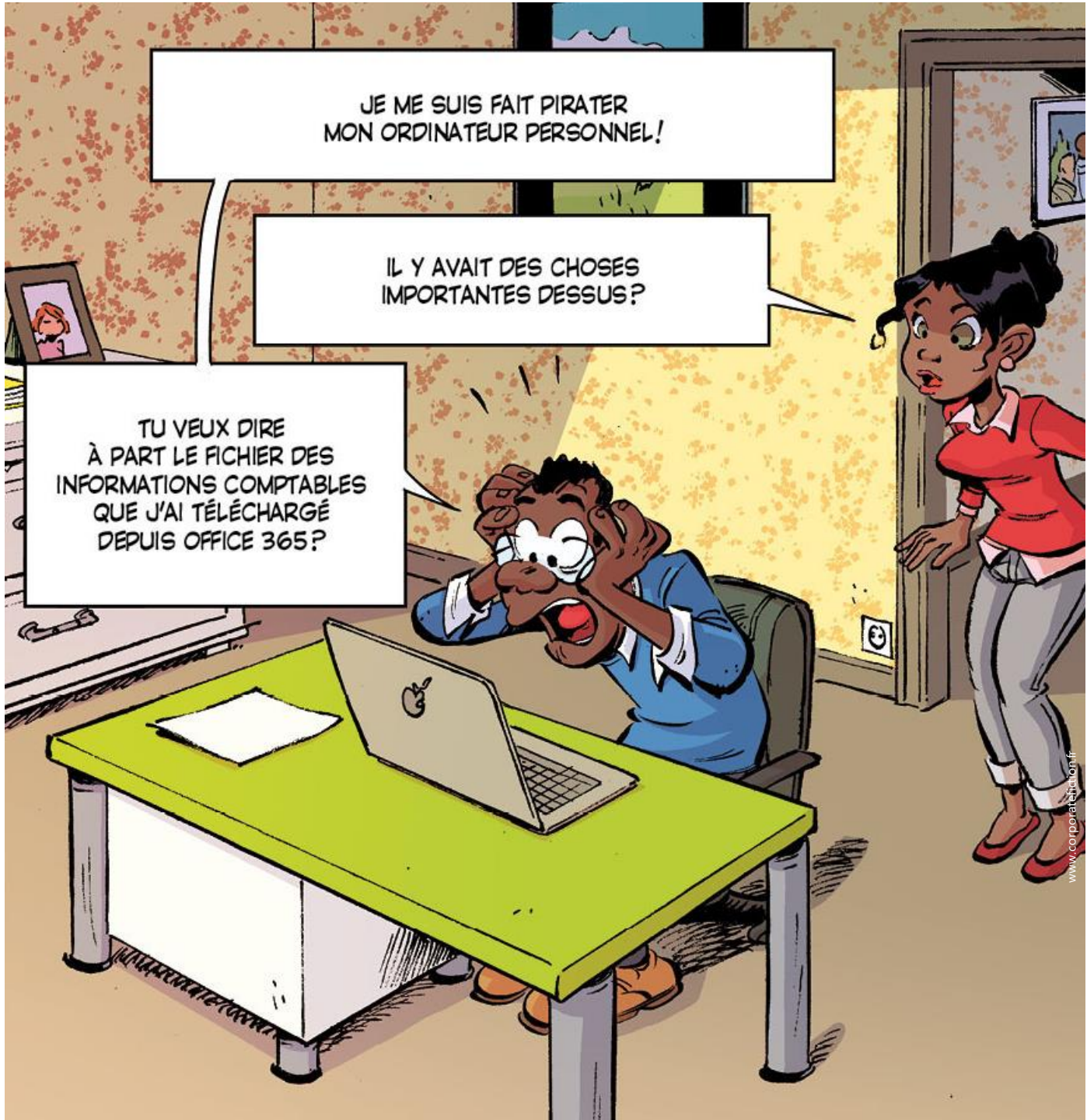
Le télétravail a renforcé les mélanges des usages professionnels et personnels.

LES BONNES PRATIQUES :

Je cloisonne strictement mes usages :

- Je n'utilise pas mon adresse email professionnelle à des fins personnelles et vice versa.
- Je limite ma navigation internet à un usage professionnel et je ne télécharge aucune application.
- Je ne stocke pas d'informations privées sur des supports de stockage professionnels.

GROUPE PASTEUR MUTUALITÉ



SENSIBILISATION À LA SÉCURITÉ DU SYSTÈME D'INFORMATION

1. Quel est le contexte ?
2. La sécurité est l'affaire de tous.
3. Les principes fondamentaux à adopter.
4. En savoir plus sur les recommandations à suivre.

GROUPE PASTEUR MUTUALITÉ

www.corporatefiction.fr – Mai 2022 – Illustrations : Léturgie

SENSIBILISATION À LA SÉCURITÉ DU SYSTÈME D'INFORMATION

EN SAVOIR +

Le **RÔLE ESSENTIEL** du comportement des collaborateurs

GROUPE PASTEUR MUTUALITÉ

www.corporatefiction.fr – Mai 2022 – Illustrations : Léturgie

MOT DE PASSE CONFIDENTIEL

Quels **risques** en cas de négligence ?

- Usurpation d'identité et actions menées à l'insu du collaborateur.

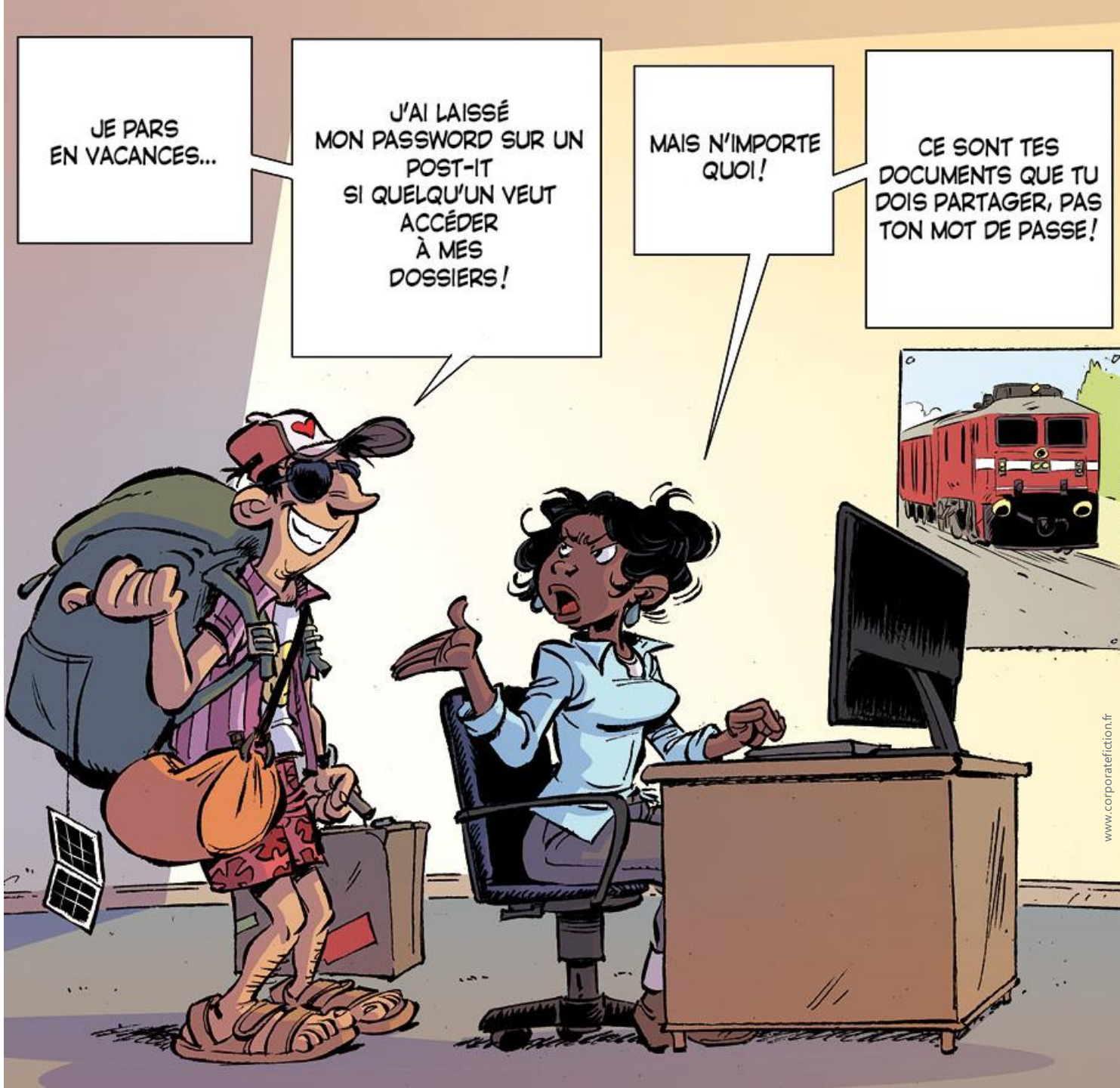
Actions mises en place :

- Renforcement du contrôle d'accès avec la mise en place de l'authentification renforcée, ce qui réduit grandement la probabilité d'une malveillance.
- Utilisation de mots complexes par les équipes techniques et stockage dans un coffre-fort numérique.

LES BONNES PRATIQUES :

- **Je ne communique mon mot de passe sous aucun prétexte**, même à ma hiérarchie ou au service informatique.

GROUPE PASTEUR MUTUALITÉ



NOUVEAUX MODES D'AUTHENTIFICATION

Quels **risques** en cas de négligence ?

- Usurpation d'identité et actions réalisées à votre insu.

LES BONNES PRATIQUES :

- **J'utilise le mode d'authentification** renforcée pour me connecter aux applications d'entreprise.
- **Je me tiens informé des dernières évolutions** de cybersécurité sur TOT'M.
- J'applique régulièrement les **mises à jour** de sécurité sur mon poste de travail et mes équipements mobiles.

GROUPE PASTEUR MUTUALITÉ

INTERNET

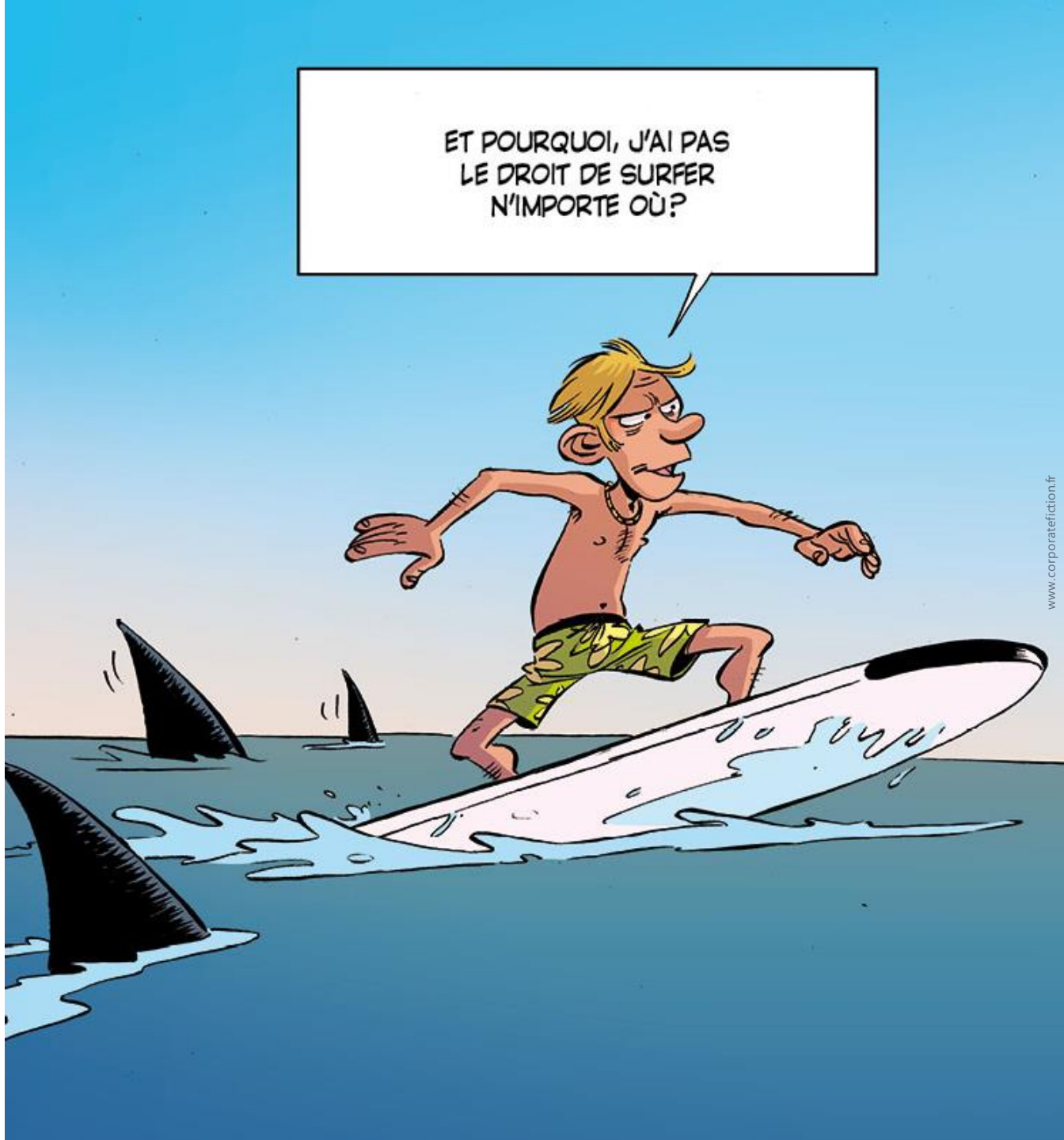
Quels **risques** en cas de négligence ?

- Contamination du système d'information,
- Vol d'identifiants ou de vos données personnelles,
- Usurpation d'identité.

LES BONNES PRATIQUES :

- **Je limite ma navigation à un usage raisonnable.**
- **Je ne télécharge aucune application sans le feu vert du service informatique.**
- **Je vérifie l'adresse URL du site** (site sécurisé en vérifiant le cadenas et l'adresse technique du site web « exemple d'URL : www.gpm.fr et non www.gmp.fr »).

GROUPE PASTEUR MUTUALITÉ



INGÉNIERIE SOCIALE

Quels **risques** en cas de négligence ?

- Faux ordres de virement,
- Usurpation d'identité ou vol de de données.

Constat :

- 33% des victimes de fraude en 2021 ont subi un préjudice supérieur à 10000€.

LES BONNES PRATIQUES :

Les techniques de fraude sont de plus en plus ingénieuses. Je redouble de vigilance face :

- Aux sollicitations douteuses (fraude au président, faux techniciens, faux placements, …).
- Aux demandes qui ne concernent pas mon périmètre ou qui concernent un collègue absent.
- Aux demandes pressantes et déstabilisantes.

GROUPE PASTEUR MUTUALITÉ

CLOUD

Quels **risques** en cas de négligence ?

- Fuite ou perte de données sensibles.

Action mise en place :

- Mise en place de la solution Oodrive pour le stockage et le partage de données, en toute sécurité.

LES BONNES PRATIQUES :

- **Je n'utilise que les solutions internes et sécurisées** pour le partage de fichiers avec un tiers, pas d'échanges de données avec les (Dropbox, WeTransfer, …).
- **Je n'envoie pas de documents confidentiels** ou de santé par mail.

GROUPE PASTEUR MUTUALITÉ

DÉPLACEMENTS

Quels **risques** en cas de négligence ?

- Fuite de données, espionnage,
- Vol d'identifiants,
- Perte de matériel.

Actions rapides :

- Identification des appareils avec des signes distinctifs ou utilisation de filtre de confidentialité.
- Mise en place d'une connexion distante et sécurisée VPN.

LES BONNES PRATIQUES :

- **Je recours systématiquement au VPN et n'utilise jamais de réseau wifi public.**
- **Je reste discret :** documents, conversations…
- Je garde mes équipements professionnels sous surveillance.

GROUPE PASTEUR MUTUALITÉ

SUPPORTS AMOVIBLES

Quels **risques** en cas de négligence ?

- Contamination ou vol d'identifiants.

Constat :

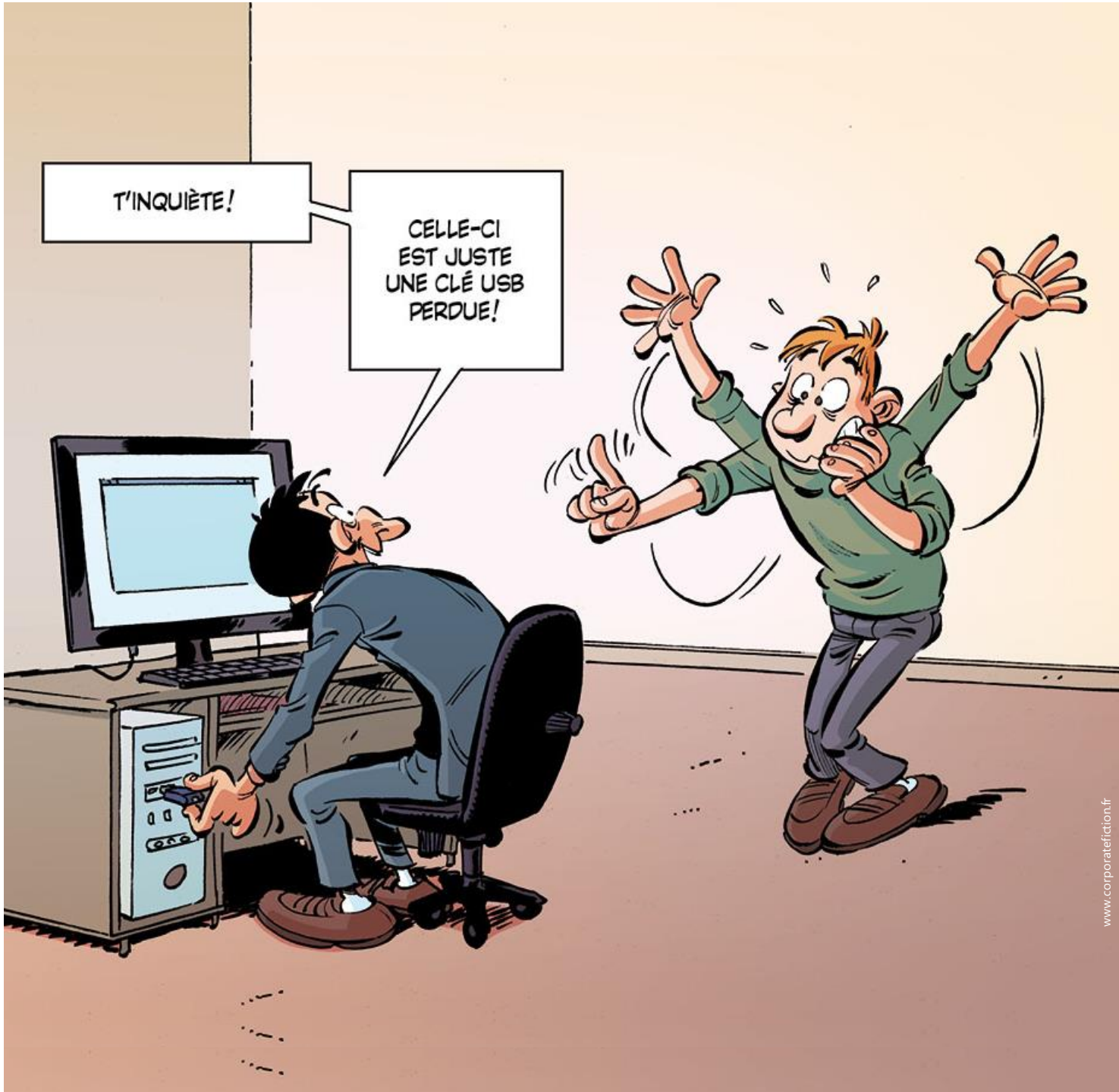
- Les clés USB trouvées sont connectées en moyenne 7 minutes après avoir été ramassées.

LES BONNES PRATIQUES :

Je refuse toute connexion de périphérique amovible sans analyse au préalable :

- Je fais analyser mon support USB par l'antivirus avant d'enregistrer des fichiers dessus.
- Si je dois utiliser un support amovible, je requiers auprès du service compétent le moyen validé et fourni par mon entreprise.

GROUPE PASTEUR MUTUALITÉ



À NOUS DE JOUER !

La sécurité est l'affaire de tous !

GROUPE PASTEUR MUTUALITÉ