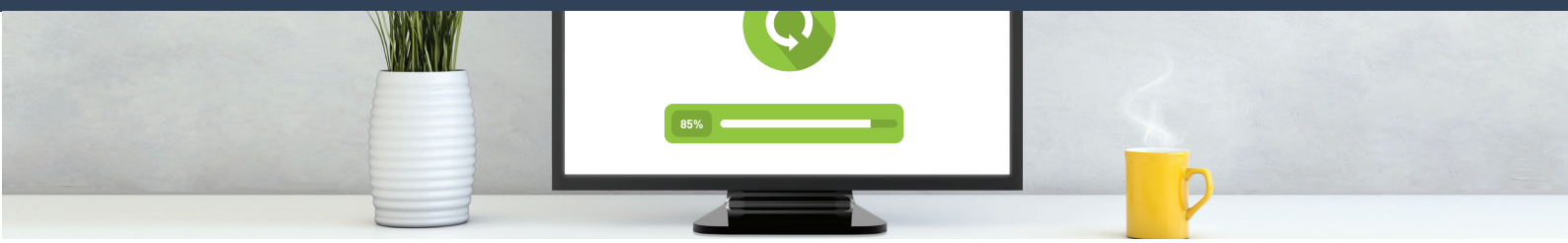
COULEUR & CONNECTION
Groupe DENTALSOFT

4 bonnes pratiques pour protéger vos données informatiques



Faites des sauvegardes fréquemment

Que vous optiez pour une **sauvegarde automatique** ou que vous choisissiez de le faire vous-même à l'aide d'un disque dur externe, veillez à **sauvegarder et protéger régulièrement vos données** (idéalement de manière quotidienne) pour ne pas faire face à un ordinateur vide suite à une attaque informatique.

Prêtez attention à vos emails

L'une des méthodes les plus couramment utilisées est la **méthode du « phishing ».** Elle consiste à faire croire à la victime qu'elle s'adresse par mail à un tiers de confiance, qu'il s'agisse d'entreprises ou d'individus (ex: les impôts, votre fournisseur d'accès à Internet, l'un de vos fournisseurs ou de vos patients...) dans le but de receuillir des informations personnelles. Ainsi, il sera souvent question, dans ces mails, de vous connecter sur un site pour divulger mots de passe, informations bancaires, etc.

Pour repérer ces mails frauduleux, plusieurs éléments peuvent vous alerter :

- **Une adresse d'expéditeur ou de nom de domaine étrange** (ex: france-impotsgouv.fr, utilisé par les fraudeurs à la place de impots.gouv.fr).
- **Des fautes d'orthographe :** un mail de la part d'EDF ou d'une boutique en ligne comprenant des fautes d'orthographe doit immédiatement vous alerter.
- **Des images ou logos dégradés, de mauvaise qualité** représentent également un bon indice de l'authenticité du mail.
- **Des moyens de paiement inhabituels demandés.**

De manière générale, **nous vous déconseillons de cliquer sur un bouton ou lien contenu dans un e-mail que vous trouvez suspect** : tapez par vous-même le nom du site internet concerné pour être sûr de ne pas être redirigé vers un site frauduleux.

Mettez à jour vos logiciels

Un logiciel qui vieillit et qui n'est pas régulièrement mis à jour peut représenter une véritable porte ouverte aux virus. N'hésitez pas à mettre à jour régulièrement vos logiciels et anti-virus, en téléchargeant au maximum **les nouvelles versions sur les sites officiels des éditeurs.**

Utilisez des mots de passe forts et variés

Vos mots de passe représentent la clé de nombreuses informations personnelles. Alors, pour éviter qu'ils tombent entre de mauvaises mains, **soignez-les** : diversifiez vos mots de passe, composez-le de lettres majuscules et minuscules, chiffres et caractères spéciaux et d'au minimum 12 caractères.
Notre astuce : n'hésitez pas à utiliser des générateurs automatiques de mots de passe en ligne tels que www.generateurdemotdepasse.com !