COVID-19
et la gestion des mots de passe

Télétravail

En cette période de COVID-19, le télétravail est d'autant plus utilisé. Mais quels sont les facteurs augmentant les risques d'attaques ?

- Laisser sa **session ouverte ou accessible**
- **Partager son mot de passe via email**, SMS, chat pour avoir accès à certains services

Attaques informatiques

Avec cette crise les entreprises sont ralenties, moins réactives et donc plus susceptibles de se faire attaquer. Quelles sont les attaques qui peuvent toucher les entreprises ?

- L'ingénierie sociale avec le **phishing**
- L'attaque par **force-brute** par des programmes testant différents logins et mots de passe, à partir de bases de données connues ou de manière aléatoire

Les bonnes pratiques

Afin d'empêcher les attaques et de renforcer la sécurité de vos outils informatiques, soyez vigilants et suivez ces bonnes pratiques :

- **Changer régulièrement** vos mots de passe pour minimiser les riques dûs à une utilisation antérieure
- Utiliser des mots de passe forts avec plus de **12 caractères**, contenant **majuscules, minuscules, chiffres et caractères spéciaux**.
- Avoir recours à la **double authentification** dès que cela est possible
- Faire l'usage de **gestionnaire de mots de passe**
- Ne pas laisser **affiché à la vue de tous les mots de passe**, par un post-it ou une étiquette sur l'écran par exemple, pratique (trop) courante dans les entreprises

Plus d'informations sur :

- www.cnil.fr
- www.ssi.gouv.fr
- www.cybermalveillance.gouv.fr

mmi BORDEAUX