# Aide-mémoire : Travail en mobilité

5 bonnes pratiques pour travailler en toute sécurité à l'extérieur du bureau!

## Faites attention à l'hameçonnage

Stratagème très utilisé par les cybercriminels surtout en temps de crise.

1. Vérifiez que le courriel est attendu et sollicité
2. Ne cliquez pas sur le lien et ne téléchargez pas les pièces jointes
3. Portez attention aux différentes situations qui tentent de vous faire réagir rapidement

## Choisissez un mot de passe robuste et unique

81% des cyberattaques utilisent des mots de passe volés ou faibles[1].

1. Créer un **mot de passe robuste** en choisissant une phrase de passe qui n'a de sens que pour vous – minimum 21 caractères Ex. jadorevivredansunetortue
2. Utiliser un **mot de passe différent** pour chaque service en ligne
3. Utiliser un **gestionnaire de mot de passe** pour les sauvegarder

## Mettez à jour vos systèmes

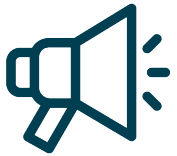
Les cybercriminels profitent grandement des vulnérabilités qui sont dans vos systèmes ou applications.

Pour être protégé, assurez-vous que le matériel qu'utilise vos employés à distance soit à jour :

- ✓ Système d'exploitation
- ✓ Applications
- ✓ Téléphone intelligent

## Mettez en place un Réseau Privé Virtuel (RPV) ou Virtual Private Network (VPN) en anglais

Pour assurer la sécurité des données qui transitent entre vos employés à distance et votre entreprise, mettez en place un réseau privé virtuel.



## Signalez toute activité suspecte

Incitez vos employés à vous signaler toute activité suspecte tel qu'un courriel d'hameçonnage, un SMS douteux ou encore un appel semblant être frauduleux, cela vous permettra de mieux anticiper les éventuels incidents de cybersécurité que pourrait subir votre organisation.

[1] Verizon's 2017 Data Breach Investigations Report

Pour en apprendre davantage, référez-vous à notre Trousse de sensibilisation à la cybersécurité