



## LES BONNES PRATIQUES À ADOPTER POUR SÉCURISER VOS DONNÉES, AU BUREAU, EN TÉLÉTRAVAIL, À DISTANCE.



### J'ADOpte UN COMPORTEMENT RESPONSABLE

Je redémarre chaque jour mon ordinateur et je m'assure que mon antivirus est à jour.

Je veille à mettre à jour les logiciels, en particulier les logiciels de sécurité, sur mes équipements, y compris tablettes et téléphones, afin de corriger d'éventuelles failles.

Je vérifie la bonne actualisation de l'antivirus et effectue les demandes de mise à jour de mon support informatique.

J'évite les sites suspects et n'installe que les applications validées par le support informatique.

Je sépare mes usages professionnels de mes usages privés



### JE SAUVEGARDE RÉGULIÈREMENT MON TRAVAIL

Je sauvegarde fréquemment mes activités sur le réseau de l'entreprise ou sur les moyens qu'elle met à disposition (clé USB, disque externe...).

1

2

3

4



### JE RENFORCE LA SÉCURITÉ DE MES CONNEXIONS

Chez moi, j'utilise un mot de passe fort d'accès à ma box et au Wi-Fi. Je vérifie que j'utilise bien le chiffrement de ma connexion en WPA2. Je redémarre ma box régulièrement pour la mettre à jour.

J'utilise des mots de passe longs et complexes, et différents pour chaque équipement et service. J'active la double authentification lorsque c'est possible.



### JE RESTE VIGILANT

Je me méfie des messages inattendus ou alarmistes par email, SMS, chat... Je demande toujours confirmation à l'émetteur par un autre moyen.

Je regarde si la provenance de l'email est sûre en scrutant son adresse et son extension.

Je ne télécharge des applications que depuis les sites ou magasins officiels des éditeurs.

Je vérifie la fiabilité et la réputation des sites que je visite.