DIRIGEANTS MAIS AUSSI UTILISATEURS.

8 BONS GESTES POUR SE PROTÉGER

ET PROTÉGER NOS DONNÉES PROFESSIONNELLES ET PERSONNELLES

1

DÉFINIR UN MOT DE PASSE DISTINCT POUR CHAQUE COMPTE

Couper les passerelles et cloisonner évite l'effet domino qui permet d'accéder à tous les comptes avec un seul mot de passe.

2

SAUVEGARDER RÉGULIÈREMENT

Conserver une copie des données est une mesure élémentaire, en entreprise comme à la maison.
Cette sauvegarde doit être indépendante afin de ne pas être touchée en cas de problème.

3

EFFECTUER LES MISES À JOUR DES LOGICIELS

C'est un principe fondamental. Les attaquants recherchent les postes dont les logiciels n'ont pas été mis à jour pour exploiter une faille non corrigée.

4

NE PAS SE CONNECTER AU WIFI PUBLIC

Privilégier une connexion 4G aux réseaux de bornes Wifi publiques, pas sécurisées : smartphones, tablettes ou ordinateurs peuvent être épiés et leurs données récupérées.

5

NE PAS TRANSFÉRER DES DONNÉES PROFESSIONNELLES SUR UN COMPTE PERSONNEL

Pour éviter toute contamination, ne pas héberger des données professionnelles sur des équipements personnels (smartphones, clé USB…), ni brancher un support personnel sur un terminal professionnel.

6

NE PAS CLIQUER SUR DES PIÈCES JOINTES, DES LIENS OU DES MESSAGES VENANT D'ÉMETTEURS INCONNUS OU NON-ATTENDUS

Même si la tentation est grande : « En cas de doute, il n'y a pas de doute ! » Un soupçon sur un message provenant d'une personne connue ? Appeler celle-ci pour confirmation !

7

ÉTEINDRE SES ÉQUIPEMENTS LE SOIR

Éteindre les terminaux limite les intrusions et fait du bien à la planète.

8

EN CAS DE SUSPICION D'ATTAQUE, SE DÉCONNECTER DU RÉSEAU

Quelque chose d'anormal se produit sur un poste de travail ? Le déconnecter du réseau pour éviter une propagation mais le maintenir sous tension pour ne pas perdre les informations utiles à l'analyse de l'attaque, et alerter les équipes de sécurité et le support informatique.