6 RÈGLES
SIMPLES ET EFFICACES
POUR ADOPTER
LA CYBER-HYGIÈNE :

1

Sensibilisez vos collaborateurs

- Menez des actions de sensibilisation avec l'appui de votre comité de direction (diffusion des bonnes pratiques, de documentation, campagnes de prévention, etc.).
- Acculturez et formez vos collaborateurs en leur proposant des formations dédiées.
- Établissez un code de bonne conduite, qui pourra prendre la forme d'une charte informatique et assurez-vous qu'il est bien assimilé par vos collaborateurs. Cette charte sera signée par chaque utilisateur lors de la remise de son matériel.
- Désignez un point de contact cybersécurité parmi vos collaborateurs qui sera l'ambassadeur des bonnes pratiques au sein de votre entreprise.
- Valorisez vos collaborateurs, faites-en les acteurs de votre cyberdéfense.

2

Gérez vos mots de passe

- Pour être efficace, un mot de passe doit être long et complexe. On évitera ceux qui peuvent être devinés facilement (« azerty », « mot de passe », etc.). Privilégiez les « pass phrases », en prenant les initiales des mots d'une phrase.
- Un mot de passe doit être individuel et rester confidentiel. Aucun interlocuteur de confiance ne vous demandera jamais de lui communiquer votre mot de passe par quelque moyen que ce soit même pour une maintenance, un dépannage informatique ou une vérification de sécurité.
- Un mot de passe différent doit être créé pour chaque usage. Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient impactés.
- Utilisez des gestionnaires ou coffres-forts de mots de passe qui vous aideront à les stocker de manière sécurisée.
- Un mot de passe doit être changé régulièrement, tous les 3 mois. En moyenne pour les services les plus critiques, un renouvellement plus fréquent est à privilégier. Celui-ci peut généralement être imposé automatiquement par certains systèmes (système d'exploitation par exemple).

3

Mettez à jour vos appareils, vos logiciels et vos antivirus

- Vérifiez régulièrement que vos appareils et logiciels ont été mis à jour et que vous utilisez bien les dernières versions disponibles.
- Lorsque votre système d'exploitation est à jour, activez les mises à jour automatiques si votre éditeur le permet.
- Installez uniquement les mises à jour proposées par votre éditeur ou fournisseur, provenant d'une source officielle fiable.
- Privilégiez deux éditeurs d'antivirus différents : un pour vos serveurs et un autre pour vos postes de travail.
- Pour vous aider dans cette action, cartographiez l'ensemble de vos appareils et de vos logiciels ainsi que leur version dans un registre. Des applications d'inventaire existent.

4

Évitez les comportements à risque

- Beaucoup d'attaquants comptent sur la curiosité et la naïveté de leurs victimes. Ainsi n'ouvrez jamais une pièce jointe suspecte ou provenant d'un expéditeur inconnu. Ne connectez jamais une clé USB en apparence abandonnée que vous auriez trouvée dans le parking ou devant l'entrée de l'entreprise car il y a fort à parier qu'elle a été laissée là intentionnellement, bien en évidence, dans l'attente qu'une future victime s'en saisisse.
- Avant de cliquer sur un lien, passez votre souris dessus pour apercevoir le nom de domaine. Ne vous aventurez pas sur des sites douteux.
- Lorsque vous êtes en déplacement, ne vous connectez jamais à un réseau public (cafés, hôtels, aéroports, etc.).
- Séparez les usages personnels et professionnels.

5

Sauvegardez !

- Réalisez des sauvegardes régulières. En cas de vol, de panne, de piratage ou de destruction de vos appareils électroniques, vous perdrez les données enregistrées sur ces supports. Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données. Identifiez les appareils et supports qui contiennent des données puis déterminez celles qui doivent être sauvegardées. Pensez également à sauvegarder les logiciels nécessaires à l'exploitation de vos données.
- Choisissez une solution de sauvegarde adaptée à vos besoins. Déterminez quelles sont les fonctionnalités nécessaires (chiffrement par exemple), l'espace de stockage requis et la facilité d'utilisation de la solution. Sachez qu'il est également possible de réaliser une sauvegarde manuelle de vos fichiers en les copiant sur un disque dur externe en veillant à les chiffrer et à les protéger par un mot de passe.
- Planifiez vos sauvegardes. La plupart des solutions de sauvegarde intègrent une fonctionnalité permettant de planifier la sauvegarde à échéance régulière. Lorsque vous l'activez, elle vous permettra de restaurer vos fichiers dans leur version la plus récente.
- Déconnectez votre support de sauvegarde de votre système d'information. S'il est corrompu, cela évitera que l'infection ne se propage à votre espace de sauvegarde. Avant de restaurer vos données il faudra vous assurer que le système d'information est désinfecté de tout logiciel malveillant.
- Protégez vos sauvegardes. Il est recommandé de conserver vos sauvegardes sur des sites différents de celui qui héberge vos données à sécuriser. Il est plus prudent de ne pas mettre tous ses œufs dans le même panier.
- Testez vos sauvegardes. Assurez-vous régulièrement que vos sauvegardes sont conformes et exploitables. Prévoyez aussi de quelle manière elles seront restaurées le moment venu en faisant des tests de restauration.

6

Mettez en place des garde-fous

- Restreignez les accès Internet uniquement aux sites nécessaires à vos collaborateurs.
- Mettez en place une politique de gestion des droits d'accès (accès informatiques mais aussi accès physiques à vos locaux en particulier pour les entrées et sorties du personnel). Il faut également prévoir une politique de mise à jour et de re-certification de ces droits.
- Sécurisez les accès wifi et utilisez un VPN pour vous connecter à distance lors de vos déplacements.
- Bloquez les ports USB de vos appareils si vous n'en avez pas l'utilité. Cela évitera à la fois d'exposer vos systèmes à une clé infectée et le vol massif de vos données par un collaborateur mal intentionné.
- Mettez en place une authentification forte multi-facteurs (confirmation d'un code reçu par SMS ou par e-mail par exemple).

POUR ALLER PLUS LOIN :
Retrouverez toutes ces bonnes pratiques ainsi que des supports de sensibilisation sur : https://www.cybermalveillance.gouv.fr/bonnes-pratiques