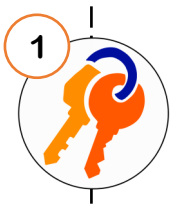
Les 12 règles d’or de la sécurité numérique

1 Choisir des mots de passe complexe

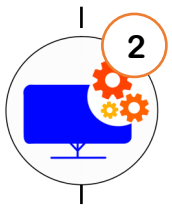
Nous vous conseillons de composer vos mots de passe en intégrant ces critères :

- Entre 8 et 12 caractères
  - ◊ Majuscules
  - ◊ Minuscules
  - ◊ Chiffres
  - ◊ Caractères spéciaux
- Aucun lien personnel
- Unique par service et par site internet



2 Mettre à jour régulièrement son poste et ses logiciels

Nous vous conseillons de réaliser régulièrement vos mises à jour principalement pour combler les failles de sécurités détectées par l’éditeur ou le constructeur.



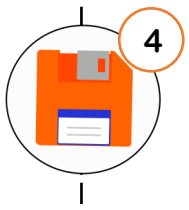
3 Attribuer les bons droits aux utilisateurs

Nous vous conseillons d’adapter les droits de chacun des utilisateurs de l’entreprise en fonction de :

- Leurs fonctions dans l’entreprise
- Leurs responsabilités dans l’entreprise

4 Effectuer et vérifier ses sauvegardes régulièrement

Nous vous conseillons de réaliser régulièrement des sauvegardes et de les vérifier pour s’assurer que l’intégralité des données soit bien présente en cas de panne. Cela nous permettra de restaurer la plus récente et ainsi vous assurer une continuité de travail.

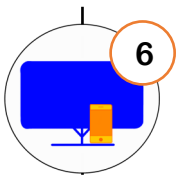


5 Sécuriser l’accès Wi-Fi de son entreprise grâce à un mot de passe sécurisé

Cependant, si vous voulez offrir la possibilité à vos utilisateurs et/ou intervenants de se connecter à un réseau internet libre et sécurisé, il existe des solutions approuvées par la RGPD que nous proposons.

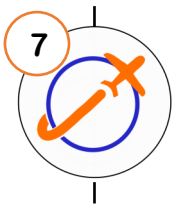
6 Être prudent avec tous vos équipements professionnels

- Installer seulement les applications/logiciels nécessaires et sécurisés
- Sécuriser leur accès avec un mot de passe sécurisé si cela est possible
- Possibilité de réaliser une sauvegarde régulière du contenu sur un support externe en cas d’obligation de restauration



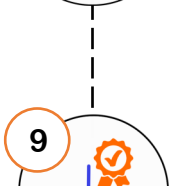
7 Protéger ses données lors d’un déplacement

- Avant de partir
  - ◊ Sauvegarder ses données
  - ◊ Installer un filtre « anti-espion » sur votre PC
  - ◊ Vérifier que vos mots de passe ne soit pas pré-enregistrés sur votre poste
- Pendant le voyage
  - ◊ Garder ses équipements et fichiers près de soi
  - ◊ Informer l’entreprise en cas de vol
  - ◊ Eviter de connecter des équipements étrangers (clé USB par exemple) à son propre équipement



8 Être prudent lorsque vous utiliser votre messagerie

- Vérifier la cohérence entre l’adresse mail et l’expéditeur
- Ne pas ouvrir les pièces jointes lorsque :
  - ◊ L’expéditeur est inconnu
  - ◊ Le titre ou le format de celles-ci est étrange ou parait inhabituelle de la part de ce contact
- Ne pas cliquer sur un lien si celui-ci est contenu dans un mail suspect
- Ne pas répondre à un mail vous demandant des informations personnelles

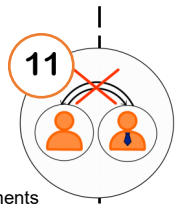


9 Télécharger ses logiciels et/ou programmes sur les sites officiels des éditeurs

Pour cela, il est important, lors du téléchargement, de décocher/désactiver toutes les cases proposant d’installer des logiciels complémentaire

10 Être vigilant lors d’un paiement sur internet

- S’assurer que le site concerné comporte la mention « https:// »
- Vérifier que l’adresse du site ne comporte aucune faute d’orthographe



11 Séparer les usages personnels et professionnels

- Ne pas transférer ses mails professionnels sur des services personnels
- Ne pas héberger de données professionnelles sur des équipements personnels
- Eviter le plus possible la connexion de support amovible personnel aux équipements de l’entreprise

12 Prendre soin des informations personnelles, professionnelles et de son identité numérique

- Être vigilant concernant les formulaires que vous êtes amenés à remplir
  - ◊ Compléter seulement les champs désignés comme « obligatoires »
  - ◊ Décocher les cases autorisant le site à conserver ou à partager vos données
- Donner accès à un minimum d’informations personnelles et professionnelles sur les réseaux sociaux
- Vérifier régulièrement ses paramètres de sécurité et de confidentialité

En appliquant ces gestes, vous protégez votre entreprise !

Ce document a été créé en suivant les directives de l’Agence Nationale de la Sécurité des Systèmes d’Information