E1. Protéger son poste de travail

Si les systèmes d'information numériques sont désormais totalement indispensables à tous les acteurs économiques, l'attention portée à leur sécurité au quotidien par leurs utilisateurs reste bien insuffisante. Les négligences sur les postes de travail exposent l'entreprise à de graves problèmes susceptibles de compromette son activité.

ORGANISATIONNEL

➤ Définir et faire appliquer une politique de choix de **mots de passe robustes**, difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne :

- au minimum 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) ;
- aucun lien direct avec la personne : éviter les noms, dates de naissance, etc. ;
- absents des dictionnaires.

➤ Définir un mot de passe unique et personnel pour chaque usage. Les mots de passe protégeant des contenus sensibles (banque, messagerie, etc.) ne doivent en aucun cas être réutilisés.

TECHNIQUE

➤ Mettre régulièrement à jour le **système d'exploitation** et les logiciels.

➤ Télécharger les installateurs de logiciels uniquement depuis les sites de leurs éditeurs et vérifier leur authenticité avant toute installation.

➤ N'installer que le strict nécessaire sur les postes de travail. En particulier, limiter les logiciels installés et les modules optionnels pour les navigateurs.

➤ Utiliser un **pare-feu** local et un **anti-virus**.

➤ Utiliser un gestionnaire de mot de passe pour leur stockage. Choisir pour ce gestionnaire un **mot de passe robuste**.

➤ Désactiver les exécutions automatiques.

➤ Chiffrer les partitions où sont stockées les données utilisateur.

➤ Désactiver les ports USB non utilisés pour la connexion des périphériques.

➤ Protéger l'accès aux informations sensibles à l'aide d'un système de contrôle d'accès adapté. Pour les informations les plus critiques, privilégier des systèmes basés sur la cryptographie comme des conteneurs chiffrés.

➤ Effectuer régulièrement des sauvegardes de données. Elles permettent de retrouver les données après une attaque (avec un rançongiciel, par exemple) ou un sinistre (incendie, inondation, etc.). Ces sauvegardes sont à appliquer en priorité aux données sensibles. Le moyen le plus sûr, mais aussi le plus simple, consiste à stocker, de manière sécurisée et dans un endroit distinct, une copie de ses sauvegardes sur un support déconnecté comme par exemple un disque dur amovible. Pour les entités plus larges où une telle solution n'est pas envisageable de manière générale, elle pourra être réservée aux données les plus sensibles.

COMPORTEMENTAL

➤ Face à un courriel suspect :
- ne jamais ouvrir les pièces jointes provenant de destinataires inconnus ou dont le sujet ou le format paraissent incohérents avec les messages habituellement reçus ;
- si des liens figurent dans le corps du courriel, vérifier l'adresse pointée par le lien avant de cliquer ;
- ne jamais répondre par courriel à une demande d'informations personnelles, confidentielles ou bancaires ;
- ne pas ouvrir ni relayer des chaînes de courriels ou des appels à solidarité suspects ;
- ne pas prendre de décisions importantes (comme un virement bancaire) sur la base d'un courrier seul.

➤ Utiliser un compte qui ne bénéficie pas des **droits** « **administrateur** » pour les tâches quotidiennes (navigation internet, usage de suites bureautiques, consultation de messagerie, etc.).

Mots clés

Mot de passe robuste : la robustesse d'un mot de passe dépend en général, d'abord de sa complexité, mais également de divers autres paramètres. Choisir des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Système d'exploitation : programme assurant la gestion de l'ordinateur et de ses périphériques.

Pare-feu : dispositif informatique qui filtre les flux d'informations entre le réseau interne et le réseau externe de l'organisme en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur.

Anti-virus : logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.

Droits « administrateur » : faculté d'effectuer des modifications touchant la configuration du poste de travail (modifier des paramètres de sécurité, installer des logiciels, etc.).

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)
- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Recommandations de sécurité relatives aux mots de passe

➤ Service du haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance.