



Charte de sécurité informatique

Pour permettre une utilisation sûre de notre site en ligne, nous nous permettons de rappeler ici quelques règles simples de sécurité informatique. Ces règles s'inspirent des règles édictées par l'ANSSI (Agence Française de l'Etat en charge de la Sécurité Informatique). La version complète est disponible ici :

<https://www.ssi.gouv.fr/actualite/charte-dutilisation-des-moyens-informatiques-et-des-outils-numeriques-le-guide-indispensable-pour-les-pme-et-eti/>

Cette charte fait l'objet d'une signature par l'ensemble des personnes participant au processus de médiation.

Règle n°1 : Respecter l'importance des mots de passe

- Interdiction de divulguer son mot de passe, il est strictement affecté à une personne ;
- Mot de passe complexe, interdiction d'utiliser les mots de passe du type "mot de passe" "password123" "123456" "654321", son nom de famille, sa date de naissance, un enchaînement de caractère sur le clavier ;
- Mot de passe composé d'au moins huit caractères, comprendre des chiffres et des lettres, au moins un caractère spécial (',@, *, ...) ;
- Renouvellement du mot de passe tous les 3 mois ;
- Interdiction de conserver des mots de passe dans des fichiers ou sur des post-it ;
- Interdiction de pré-enregistrer les mots de passe dans les navigateurs.

Règle n°2 : Les logiciels utilisés

- Exclusivement utiliser le site officiel de l'éditeur pour télécharger un logiciel ;
- Configurer les logiciels pour installer automatiquement les mises à jour. Si ce n'est pas possible, télécharger les correctifs de sécurité disponibles.

Règle n°3 : Pour les ordinateurs portables et les smartphones

- N'installer que les applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...) ;



- En plus du code PIN qui protège votre carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement ;
- Éviter de le laisser sans surveillance ;
- Verrouiller les applications et outils sensibles ;
- Veiller à saisir son mot de passe avec discrétion.

Règle n°4 : Règle d'utilisation de la messagerie

- Ne pas ouvrir les pièces jointes provenant d'expéditeurs inconnus ;
- Ne pas cliquer sur un lien figurant dans un e-mail trop rapidement, si vous ne l'attendiez pas ;
- Ne jamais transférer par mail des codes confidentiels ou des numéros de carte bancaire, et de façon générale des données personnelles ;
- Ne pas relayer de chaînes d'alerte, d'appels à la solidarité, d'alertes virales ;
- Ne pas faire suivre vos messages professionnels sur votre messagerie personnelle.

Règle n°5 : Lors d'un paiement d'un Internet

- Vérifier la réputation du site ;
- Contrôler la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet ;
- assurez-vous que la mention « https:// » apparaît au début de l'adresse du site Internet.

Règle n°6 : Les clés USB, les disques durs externes

- Ne pas utiliser des clés USB ou des disques durs externes personnels sur différents ordinateurs ;
- Vérifier la provenance d'une clé USB fournie, elle peut contenir un virus.

Règle n°7 : Les antivirus

- Installer un antivirus reconnu ;
- Vérifier que la mise à jour automatique a bien été activée.



Règle n°8 : La sécurité des accès wifi

- Sécuriser l'accès à votre wifi, en modifiant le code d'accès à votre wifi (souvent inscrit sur la borne d'accès à internet) par un code de plus de 20 caractères ;
- Vérifier que la borne dispose d'un protocole de chiffrement et qu'il est bien activé.
- Éviter de se connecter à un wifi public.