



# 8 règles d'hygiène informatique que l'on devrait tous respecter

La sécurité informatique et la protection des données stratégiques, c'est d'abord **des gestes simples au quotidien**. Vous trouverez ci-après une liste (non exhaustive) de 8 bonnes habitudes à adopter pour prévenir les mauvaises surprises qui peuvent coûter cher.

## 1. Choisissez des mots de passe robustes

Évitez les mots de passe trop simples avec des combinaisons trop basiques, de type prénom et date de naissance, facilement piratables. Essayez autant que possible de ne **jamais utiliser le même mot de passe**.

## 2. Mettez à jours vos systèmes d'exploitation, vos logiciels et vos antivirus

Les menaces se renouvelant sans cesse, pensez à bien **mettre à jour vos outils**.

## 3. Effectuez des sauvegardes régulières

Parce que **la panne de disque dur n'arrive pas qu'aux autres**, faites des sauvegardes régulières afin de ne pas perdre des données cruciales à l'activité de votre entreprise.

## 4. Sécurisez votre point d'accès Wi-Fi

**Ne laissez pas à la portée de tous** l'accès à votre Wifi et protégez-le d'un mot de passe complexe. Voir la bonne pratique n°1 !

## 5. Soyez prudent lors de l'ouverture d'un e-mail

En cas de doute sur la provenance, la l'objet ou le contenu d'un e-mail, **ne prenez aucun risque et détruisez le** et les pièces jointes associées. Nous vous avons d'ailleurs alerté dans des précédents articles sur [les escroqueries au « faux RIB »](#) ou « [par faux technicien](#) » dans un [précédent article](#) ou encore de la [recrudescence des campagnes de courriels piégés à l'aide de malwares "macros"](#).

## 6. Téléchargez les programmes et logiciels directement sur le site des éditeurs

Lorsque vous souhaitez télécharger un nouveau logiciel sur votre ordinateur, **privilégiez toujours les sources sûres** comme les sites des éditeurs de ces mêmes logiciels.

## **7. Soyez vigilant avant d'effectuer un paiement sur internet**

Dès que vous effectuez des transactions sur Internet, vérifiez que l'url est bien en "https" et non en "http", ce qui garantit la sécurité et la confidentialité des coordonnées bancaires. Même chose que pour les e-mails, **au moindre doute sur la fiabilité de la plateforme d'achat, faites sens inverse.**

## **8. Prenez soin de vos informations personnelles et de votre identité numérique**

Faites attention à **la diffusion de vos données personnelles**, notamment sur les réseaux sociaux, qui pourraient nuire à votre image et à celle de votre entreprise.

Pour aller plus loin vous pouvez consulter la [fiche de l'Agence nationale de la sécurité des systèmes d'information \(ANSSI\)](#). Les points évoqués ci-dessus y sont développés.