

## Pourquoi ma p'tite entreprise, n'est pas à l'abri d'aucuns risques numériques ?



*L'informatique est un outil utilisé progressivement et dorénavant de façon importante dans les entreprises. Englobé dans la thématique numérique, l'usage généralisé des produits et services ne s'avère pas sans risques.*

**Ce sont les conséquences potentielles de ces risques numériques, qui sont très souvent ignorées.**

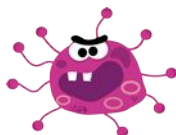
**Cela peut s'avérer catastrophique** pour une entreprise ou toutes autres structures et peu importe son secteur d'activité, sa taille, ... Car tout le monde est ciblé aujourd'hui ! Des entreprises ont déjà mis fin à leurs activités, du fait des conséquences d'un risque numérique. Comme une attaque par rançon-logiciel et **à minima perdra beaucoup d'argent**. Car **remettre en état le système peu s'avérer coûteux**, très coûteux.



Plus grand monde ne pourrait se passer d'Internet, de la messagerie, de son Smartphone, ..., pour travailler, dans le cadre d'un usage plus ou moins professionnel. Hors, tous ces outils comportent des faiblesses, des failles, ... Et c'est très souvent au travers de nos usages, car **l'humain en est le maillon faible**, que les risques prennent vites formes.



**En prendre conscience est essentiel, agir est vital, ... Pour éviter des catastrophes, pouvant mener à engager la pérennité de l'entreprise ! Croire qu'en tant que petite structure, vous êtes à l'abri est une erreur fondamentale !**



**Mais plus de 80 à 90 % des risques, peuvent être couverts par la mise en application des bonnes pratiques d'hygiène numérique.** Que vous pourrez éventuellement compléter par une assurance spécifique. Ce qui vous permettra de couvrir certains coûts liés à la remise en état du système numérique atteint. Toutefois, de plus en plus, le prix et la franchise de ce type d'assurance dépendra de ce que vous aurez fait pour éviter les risques. Car comprendre que se protéger à 100 % est plutôt un vœu pieux, les compagnies d'assurances imposeront de surcroît des audits.



**Les bonnes pratiques d'hygiène numérique** sont l'application des règles suivantes :

- Gestion des mots de passe ;
- Sauvegarde des données et systèmes ;
- Appliquer les mises à jour ;
- Protéger ses équipements ;
- Gérer correctement sa messagerie.

*Sensibiliser collaborateurs et dirigeants est un enjeu essentiel et collectif, pour que tout le monde joue selon les mêmes règles. Le maillon faible en matière d'hygiène numérique étant l'humain, car ce n'est jamais la machine qui fait des erreurs.*



Pour cela, sont à disposition des entreprises, un certain nombre de ressources proposées entre autres par l'**ANSSI (Agence Nationale de Sécurité des Systèmes d'Informations)** et **Cybermalveillance**. Les institutions représentatives apportent également leurs pierres à l'édifice en matière d'hygiène numérique. En proposant, par exemple des sessions d'information et outils documentaires.



L'un des principaux concepts en matière de sécurité numérique est de base d'empêcher l'accès aux systèmes. Ce qui veut dire en claire, que l'on applique par défaut la règle qui est d'en fermer totalement les accès.

Beaucoup d'équipements, de services ont un usage au travers d'identifiants et mots de passe. On s'attachera donc, lors de leurs mise en service à changer ces derniers. Très souvent définis par défaut et très probablement connu d'individus pouvant vouloir agir avec malveillance.

Comme nous l'avons dit plus haut c'est en appliquant les bonnes pratiques d'hygiène numérique recommandées. Que nous allons détailler ci-dessous. Que l'entreprise se protégera contre plus de 80 % des risques, auxquels elle peut étre confrontés.

Ainsi chaque point détaillé ci-dessous est essentiel et participe à une protection globale :

◆ La gestion des mots de passe :

Aujourd'hui, l'usage d'outils numériques implique l'utilisation de mots de passe, très souvent associés à une adresse courriel. La pratique c'est d'avoir un mot de passe unique pour chacun. Utilisant une chaîne de caractère alphanumérique avec caractères complexes. Naturellement, on utilisera un gestionnaire sécurisé pour cela, comportant un générateur ;

◆ La sauvegarde des données et systèmes :

Sauvegarder ses données est essentiel. Il faut s'assurer que celles-ci puissent être restaurées. La règle absolue est de le faire en trois exemplaires, tous les jours, toutes les semaines, tous les mois, trimestres et années. En cas d'utilisation d'un service de sauvegarde en ligne, on portera une vigilance accrue à la capacité de restauration des données ;

◆ L'application des mises à jour :

Aucun écosystème numérique ne peut être considéré sur le plan fonctionnel et sécuritaire comme fiable à 100 %. L'application des mises à jour est donc essentiel et participe globalement à la protection de vos systèmes numériques ;

◆ La protection de ses équipements :

Comme dit plus haut aucun équipement numérique ne peut prétendre à une fiabilité et sécurité à 100 %. D'autant plus qu'il est à considérer que le maillon faible, c'est l'humain. Nos usages nous poussent à échanger des fichiers au travers de la messagerie, de médias, ... Ces fichiers peuvent être infectés (logiciel malveillant, virus, ...). Il est donc essentiel que les équipements soient protégés avec des outils de sécurité suffisamment performant mais, pas trop invasifs tout de même. L'équilibre est subtil mais essentiel et l'anti-virus ou l'anti-malware devront être assez performant tout en sachant se faire oublier ;

◆ Utiliser correctement sa messagerie :

La messagerie est le vecteur par excellence de diffusion des menaces. Entre les indésirables (spams), les courriels d'hameçonnage (phishing), ... Il est clair que l'utilisateur est confronté dans ses usages, surtout si son adresse courriel circule. L'utilisation de formulaire de contact est ainsi préférable à la diffusion d'une adresse sur son site Internet. L'utilisation d'une adresse dédiée éventuellement chez un hébergeur générique, pour les réseaux sociaux est une autre piste. De façon plus générale on veillera au bon fonctionnement de l'anti-spam. De l'application de règles simples permettant d'éviter l'ouverture de courriels infectés, par exemple.



Le monde de l'entreprise est également friand des réseaux sociaux. Leurs usages à des fins commerciales ou pour recrutement, c'est fortement développé ces dernières années. Le corollaire, c'est qu'aujourd'hui les individus malveillants, appartenant de plus en plus à des réseaux criminels, exploitent eux aussi les réseaux sociaux. Ainsi que les informations qu'ils contiennent. Menant par exemple à de très nombreuses tentatives d'escroqueries, comme l'arnaque au président ou celle au faux RIB fournisseur.

On pourra ainsi éviter l'ingénierie sociale, en :

- **limitant les informations diffusées sur les réseaux sociaux** ;
- **mettant en place des procédures de contrôles** en escalades ;
- attirant la vigilance des collaborateurs.



Cela n'a rien de technique mais, fait partie des bonnes pratiques au sein de toutes les organisations pour couvrir tous les risques. Complété d'une charte d'utilisation des outils numériques que les collaborateurs de l'entreprise signeront.



L'aspect juridique s'est invité dans la partie, avec l'entrée en vigueur en 2018 du Règlement Général sur la Protection des Données (RGPD). Même s'il existait déjà la loi dite « Informatique et liberté » de 1978.

**L'entreprise prend encore plus de risques, financier entre autres du fait des amendes possibles. À ne pas faire le nécessaire, pour se protéger.**



De façon générale, avoir ses données stockées de façon centralisée et sécurisée est un atout. Car la sauvegarde en est facilitée. Multiplier l'éparpillement des données au travers d'outils bureautiques, certes essentiels dans les organisations, est un risque que l'entreprise ne peut plus se permettre de prendre. L'usage d'un PGI (Progiciel de Gestion Intégré) outre les fonctionnalités qu'il apporte, peut permettre justement l'application des bonnes pratiques et faciliter celle du RGPD.



**Aucune entreprise n'est aujourd'hui à l'abri face aux risques numériques.** C'est par l'application collective des bonnes pratiques d'hygiène numérique, quelle se protégera. **Le dirigeant, l'entrepreneur et ses collaborateurs, quand il en a, doivent en prendre conscience.** L'accompagnement est essentiel, car entre le RGPD, les assurances et l'aspect technique de la thématique, l'artisan, commerçant, ..., ne peut les maîtriser.

Maintenant que vous avez compris que **rien ne vous protège**, ne tardez pas à engager les actions qui vous permettront de l'être. Car avec un peu de bon sens et quelques principes simples, appliqués par itérations. Vous éviterez progressivement bien des problèmes. Dans le pire des cas, il vous faudra porter plainte, faire appel aux spécialistes pour la conservation de la preuve et la remédiation. Mais la notion essentielle à comprendre, c'est que **la prévention est bien moins coûteuse qu'une action curative** !