

Et si votre réussite était aussi matérielle ?

Choisir le bon matériel informatique peut relever du casse-tête. PC ou Mac ? Matériel fixe ou mobile ? Couplé avec votre smartphone, ou indépendant ? Autant de questions auxquelles votre prestataire informatique devra répondre pour vous permettre un réel gain de productivité adapté à votre activité et votre développement. Chaque entreprise représente un microcosme dont les besoins et les attentes sont spécifiques. Il est donc indispensable de se faire accompagner par un spécialiste qui saura vous conseiller et vous guider dans votre choix. Ce n'est pas pour rien que l'on parle de parc informatique. Un parc se compose de plusieurs espaces différents et complémentaires. Dans une imprimerie par exemple, la personne en charge de lancer les impressions, n'a pas les mêmes besoins que la personne responsable de la comptabilité. Auditer le besoin en amont permettra de répondre à vos besoins et donc de permettre d'avoir un environnement informatique performant. N'hésitez pas à comparer les propositions car votre prestataire informatique deviendra vite votre allié. Outre le manque de connaissance,



dans ce domaine, qui peut être un frein pour certains dirigeants, le coût peut aussi être une raison pour retarder le renouvellement du parc. Or, il existe des solutions comme le leasing (location du matériel avec option d'achat) ou l'infogérance (délégation des tâches informatiques à un spécialiste) qui permettent de lisser le coût d'équipement et d'entretien informatique. Avoir recours à ces options permettra d'avoir un équipement neuf, à jour, et régulièrement renouvelé. Cette solution est de plus en plus plébiscitée par les automobilistes, alors pourquoi les professionnels ne pourraient pas faire de même avec leur parc informatique ?

LES NEWS ADEO

Magazine n°1 - Adeo-informatique | adeo-informatique.fr | 04 688 24 688

Et si nous avions pu éviter ce drame ?

Le 15 avril 2019, Notre Dame de Paris, l'un des symboles les plus importants de notre patrimoine, est partie en flammes. En une étincelle, c'est une charpente de 800 ans qui s'est vue partir en fumée. Au-delà de la perte inestimable, et de la question de la reconstruction qui est sur toutes les lèvres, nous sommes en droit de nous poser cette question, commune à toute type d'accident : ce drame aurait-il pu être évité ? À l'image de Notre-Dame, bon nombre d'entreprises, notamment les PME, voient leur patrimoine informatique être attaqué. Cela n'arrive pas qu'aux autres.



adeoⁱⁿ

Vous souhaitez un **diagnostic informatique** ?
Ayez le réflexe Adeo.

Je demande un devis

Tél : 04 688 24 688 - adeo-informatique.fr
Perpignan | Mas Guérido



Qu'il s'agisse de dégâts matériels, humains, appliquer des normes de sécurité, peut-il nous mettre à l'abri ? Sur l'année 2018, 21% des PME françaises ont été victimes de cyber-attaques. Le coût de ces attaques oscille entre 10 000 et 100 000 euro selon les cas. Certaines entreprises ne sont pas en mesure de se remettre de ces attaques. Elles sont donc à prendre en compte dans les menaces que courent votre entreprise, au même titre que les nouveaux concurrents sur votre marché.

Il ne s'agit pas ici de se laisser gagner par le catastrophisme, mais juste d'être conscients du danger. Les principaux dangers que les entrepreneurs craignent sont : le piratage de leurs données, les emails frauduleux, le vol du matériel informatique, l'escroquerie et enfin les virus. Face au danger, il est donc logique de se protéger et d'être bien accompagné.

Chacun d'entre eux peut-être évité avec l'équipement et les conseils adéquats : serveur sécurisé, pare-feu, maintenance... sont les garants d'une infrastructure informatique fiable et sécurisée. Cependant, chaque infrastructure d'entreprise a ses spécificités, ses besoins. Un spécialiste du secteur saura vous indiquer ce qui est le plus adapté à votre entreprise. De telles précautions en amont reviennent à installer un détecteur de fumée pour éviter d'avoir à éteindre un terrible incendie...

LES BONNS CONSEILS ADEO INFORMATIQUE

- 
1 Sauvegarder régulièrement les données de votre entreprise.
- 
2 Sécuriser les mots de passe
- 
3 Changer régulièrement les mots de passe
- 
4 Faites les mises à jour de votre ordinateur et des logiciels régulièrement
- 
5 Former tous les salariés

ADEO
© Copyright - Adeo-informatique
www.adeo-informatique.fr

La meilleure des défenses, c'est l'attaque. Ayez les clés pour l'éviter et la gérer.

Au quotidien, il nous paraît naturel de faire preuve de prudence pour éviter les situations à risque. Nous vous indiquons comment faire de même dans votre quotidien professionnel sur votre réseau informatique. Ces bonnes pratiques sont simples.

- Sauvegarder régulièrement les données de votre entreprise. Cette sauvegarde vous sera vitale si jamais vous perdiez les données de votre entreprise. Elle vous permettra de rétablir tout votre historique comme lors de la dernière sauvegarde.

- Sécuriser les mots de passe. Ils sont la porte d'entrée de chacun des terminaux (fixes et mobiles) de l'entreprise. Si on trouve la clé, on a donc accès à l'entreprise et ses données par le biais de l'un de ses ordinateurs. Il est donc préférable d'éviter des mots de passe simples : un prénom, une date, un lieu qui vous est proche. À l'ère des réseaux sociaux, ces données sont de plus en plus accessibles au plus grand nombre. Un mot de passe sécurisé, sera donc le meilleur allié de chacun des salariés en terme de sécurité. Il existe des systèmes générant des mots de passe ultra sécurisés.

- Changer régulièrement votre mot de passe. Il est certes important d'avoir un mot de passe sécurisé, mais le changer de façon régulière vous permettra de redoubler de précaution. Gardez bien au chaud l'outil

qui vous permet de générer des mots de passe, il vous sera utile tous les deux mois.

- Mises à jour. On a tendance à repousser les mises à jour proposées par nos ordinateurs (PC ou Mac cela ne change rien) car elles supposent de redémarrer le matériel. Or, l'une des premières finalités de la mise à jour est de réduire les failles de sécurité. Profitez donc de cette pause pour discuter entre collègues pendant que votre ordinateur se met à jour. Cette pause sera doublement utile.

- Former tous les salariés. Il est primordial de sensibiliser l'ensemble des salariés à la question de la sécurité informatique. Consacrez une formation sur ce sujet pour vos équipes ceci leur permettra d'assimiler la bonne conduite à adopter en amont et en cas d'attaque.

Vous voilà prêts pour protéger vos données de façon simple. Ces bonnes pratiques sont bien entendu complémentaires avec une infrastructure fiable et sécurisée. Avec la bonne conduite et les bons outils, les hackers peuvent passer leur chemin...