

NOUS AIDONS LES ENTREPRISES À TRANSFORMER
LEURS TECHNOLOGIES EN LEVIER D'AFFAIRES

CONSEIL EN SÉCURITÉ-TI

Ne vous contentez pas
seulement de fermer
votre fureteur...



Lorsque vous accédez à votre compte bancaire en ligne (ou autres sites avec des informations sensibles), **assurez-vous de fermer votre session et ENSUITE de fermer votre fureteur.** Si vous fermez seulement ce dernier sans vous déconnecter, certaines informations de votre session sont toujours en cours d'exécution en arrière-plan et un pirate pourrait les utiliser pour avoir accès à vos données.

Pour d'autres conseils en sécurité, **téléchargez gratuitement notre rapport 7 protections critiques essentielles en TI** au www.ars-solutions.ca/protectionscritiques

Suivez-nous



5 raisons avantageuses d'impartir vos TI



que vous ayez ou non une ressource technique à l'interne

Pour des entreprises de 100 employés et moins, il est beaucoup plus avantageux d'impartir intégralement les TI que d'embaucher une ressource à temps complet dû au fait que vous faites affaire avec une équipe spécialisée ayant les outils et les compétences nécessaires vous apportant un **meilleur rapport coûts/bénéfices.**

VOICI 5 RAISONS STRATÉGIQUES D'IMPARTIR VOS TI :

1 Gérer des TI demande beaucoup de temps: **coordination, implication et gestion. Et plus que ce qu'on peut imaginer.** En déléguant la gestion et la coordination de vos TI, **vous récupérez du temps pour toutes vos activités.** Vous n'aurez pas à vous occuper d'embaucher ou de remplacer une ressource en cas de départ, d'encadrer votre dossier informatique en général, de suivre les différents intermédiaires, etc. Toutes des tâches que vous pourrez facilement éviter en externalisant vos TI.

2 **Que vous ayez ou non une ressource à l'interne, vous préviendrez la détérioration de vos systèmes en confiant à votre fournisseur de services TI les tâches plus « cléricales ».** Elles sont souvent négligées lorsqu'une seule ressource doit tout faire et qu'elle est bombardée de demandes usagers et de projets ponctuels de toutes sortes. Les tâches telles que la surveillance de vos systèmes, les vérifications mensuelles de sécurité, de performance et de stabilité de votre environnement, **sont primordiales pour la continuité de vos opérations.** Bien que routinières et souvent déplaisantes pour votre ressource technique qui a soif de projets, ces tâches doivent être faites avec assiduité et minutie si vous ne voulez pas que votre environnement ne se détériore.



SUITE À LA PAGE 2 ▼



SUITE DE LA PAGE 1 ▲

5 Vaut mieux régler les problèmes à la source et stabiliser votre environnement avant d'embaucher. Non seulement l'embauche ne sera probablement plus nécessaire, mais vous gagnerez également en productivité et satisfaction de votre personnel.

Souvent, on pense faire une économie en embauchant quelqu'un qui devra pratiquement faire les tâches d'un département au complet: programmation, administration du réseau, support aux usagers... C'est malheureusement impossible. Chacun a sa propre spécialité. **L'entreprise demeure à risque si elle dépend d'une seule personne...**

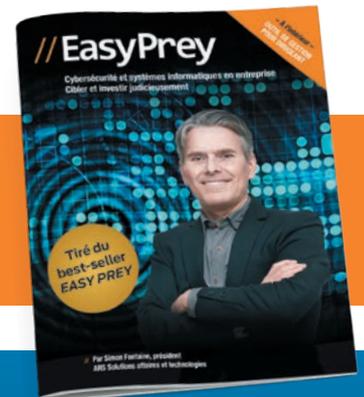
Il existe plusieurs modèles d'impartition. Le fournisseur doit proposer le modèle qui convient le mieux selon les besoins du client. Veut-on de la maintenance et de la proactivité ou gérer à la demande ?

3 En ayant accès à une équipe multidisciplinaire, vous ne serez plus dépendant d'une seule personne qui détient toute la connaissance de vos systèmes. Vous aurez ainsi un « Plan B » en cas de départ de votre ressource, maladies, vacances, etc. Impartir devient votre police d'assurance en plus de vous amener une vision globale et une **paix d'esprit**.

4 En faisant l'étape 2, vous améliorerez la rétention et la motivation de votre personnel – sujet régulièrement soulevé lors de Plans Directeurs. Investir du temps de votre ressource dans des projets pour votre entreprise (programmation d'une application stratégique pour vos opérations, implantation d'une technologie en lien avec vos objectifs de croissance, etc.).

Simon Fontaine, Président
simon.fontaine@ars-solutions.ca

Un outil stratégique extrêmement efficace pour votre comité de gestion



OFFRE DE LANCEMENT !

Nous vous offrons une rencontre de 2 heures avec Simon Fontaine, coauteur de deux best-sellers en technologies pour vous aider à faire l'exercice

ET

Une validation de la sécurité des éléments ciblés comme étant essentiels

GRATUIT (valeur de 795 \$)*

Cet exercice vous aidera à...

- Découvrir des informations cruciales à sécuriser dont vous n'étiez pas au courant;
- Assurer la continuité de vos affaires;
- Ramener le pouvoir vers vous, en ayant les outils requis.

Pour bénéficier de cette offre, contactez-nous au 418 872-4744 ou écrivez directement à simon.fontaine@ars-solutions.ca

Pour en savoir plus:
ars-solutions.ca/lancement

Comment retenir tous ses mots de passe ?

Considérant la quantité de comptes en ligne que nous avons : services bancaires, applications, intranet, médias sociaux, etc., il peut devenir assez fastidieux de se rappeler de tous ses identifiants et mots de passe. Pas étonnant que plusieurs d'entre nous soient tentés de les réutiliser un peu partout. Toutefois, il est recommandé d'avoir des **mots de passe variés et complexes**. Mais qui dit complexes, dit plus difficile de s'en rappeler...

Pour contrer ce problème, les experts en sécurité encouragent l'utilisation d'un **gestionnaire de mots de passe**. Il s'agit d'un logiciel ou service en ligne qui permet à un utilisateur de centraliser l'ensemble de ses identifiants et mots de passe dans une base de données accessible par un mot de passe unique, afin de n'en avoir plus qu'un seul à retenir. **Par contre, est-ce vraiment sécuritaire d'utiliser ce genre de service ?**

COMMENT CHOISIR SON MOT DE PASSE ?

- Ne réutilisez pas vos mots de passe. Même le plus complexe ne sera pas sécuritaire si quelqu'un le trouve.
- Bien qu'il soit conseillé d'utiliser en alternance une combinaison de majuscules et de minuscules avec des nombres pour modifier un mot (par exemple: BoNjOuR123), ces mots de passe sont plus facilement piratés que vous ne le pensez.
- Un bon mot de passe devrait contenir au moins **huit caractères (ou plus) et un mélange de lettres majuscules et minuscules ainsi que des chiffres et des caractères spéciaux (!,?,#,\$)**.
- Il est recommandé de prendre une phrase inoubliable et inutile comme « Je suis un géant de métal de 7 pieds de haut » et d'utiliser la première lettre de chaque mot avec la ponctuation suivante : « Jsugdmd-7pdh ».
- La meilleure façon de vous protéger est d'utiliser l'authentification à 2 facteurs, qui vous enverra un message avec un code ou utilisera une application pour vérifier votre connexion.

LES MEILLEURS GESTIONNAIRES DE MOTS DE PASSE

LastPass...

dashlane



Bien qu'il existe beaucoup d'options sur le marché, votre choix devrait s'arrêter sur un gestionnaire de mots de passe **sérieux, qui fait preuve de transparence avec ses utilisateurs** en les avisant rapidement si un problème est détecté.

Malgré les craintes que certains ont à propos de leur utilisation, **les experts en sécurité conviennent que les gestionnaires de mots de passe sont encore le moyen le plus sécuritaire de sécuriser ses comptes en ligne**. Toutefois, ceux qui sont basés sur votre navigateur Web ne doivent pas être utilisés. Ils sont très risqués et ont le potentiel de faire en sorte que vos informations d'identification peuvent être volées sans que vous en ayez connaissance si vous visitez un site malveillant ou cliquez sur une publicité frauduleuse.



TOP 10 DES MOTS DE PASSE LES PLUS UTILISÉS ET À ÉVITER

- | | |
|-------------|--------------|
| 1. password | 6. 12345 |
| 2. 123456 | 7. dragon |
| 3. 12345678 | 8. pussy |
| 4. 1234 | 9. baseball |
| 5. qwerty | 10. football |

TRUCS COMMUNS UTILISÉS POUR VOUS ARNAQUER...

- La banque ne vous contactera jamais pour connaître votre code PIN ou votre mot de passe.
- Aucune compagnie n'ira chez vous pour vous collecter des informations financières ou même vous demander votre carte bancaire.
- Aucune entreprise ou individu ne doit connaître vos informations financières personnelles, y compris la banque ou la police. Ne divulguez en aucun cas votre NIP, mot de passe ou vos données personnelles, sauf si vous êtes certain de savoir à qui vous vous adressez.
- N'assumez pas qu'une personne qui vous contacte par téléphone est fiable si elle connaît des informations personnelles sur vous. Cela pourrait avoir été recueilli ailleurs ou reconstitué par d'autres moyens.



Faire exploser sa productivité en suivant la routine simple de Kevin O'Leary

Comme vous pouvez l'imaginer, Kevin O'Leary – la vedette de Shark Tank et des Dragon's Den, est plutôt occupée. Le multimillionnaire accompli mentionne que son téléphone « sonne à peu près toutes les 30 secondes » et que sa boîte de courriel déborde, mais ça, il s'en fout...

« Pas jusqu'à ce que j'atteigne les trois objectifs quotidiens que je me suis fixés la nuit précédente » a-t-il récemment déclaré au magazine *Entrepreneur*. « **Chaque tâche doit être accomplie avant de prendre des appels ou d'envoyer des courriels.** Et je suis strictement ce processus simple quotidiennement, et ce, sans exception, sauf lors d'une urgence catastrophique », mentionne l'entrepreneur de 62 ans.

« Qu'il s'agisse de la famille ou du travail ou de quelque chose de personnel, je ne travaille sur rien d'autre, peu importe de quoi il s'agit. Jusqu'à ce que ces trois objectifs soient atteints, j'ai l'attitude suivante: personne ne peut avoir mon temps ou mon attention ».



Il y a une raison pour laquelle O'Leary – a.k.a. « Mr. Wonderful », réduit sa journée à trois priorités prédéfinies. Tel un café qui vous donne un élan d'énergie, « cela me rend très, très productif. J'évite tout bruit, j'accomplis les trois tâches et je continue ma journée ».

Il souligne que s'il est tentant de vouloir réaliser plus de trois tâches obligatoires chaque matin, vouloir en faire plus peut conduire à l'échec. « Soyez réalistes. Ne vous surchargez pas... trois c'est suffisant », souligne-t-il.

Solutions Cloud

Comment le *Machine Learning as a Service (MLaaS)* transformera votre entreprise ?



Le *Machine Learning as a Service (MLaaS)* est un service Cloud en pleine effervescence qui permettra d'analyser différentes données basées sur des *patterns* et de les faire concorder en extrayant des comportements cachés. **Le tout servira à prendre de meilleures décisions.** Dans une réalité où tout est de plus en plus connecté (IoT) et où de plus en plus de données sont amassées, le *Machine Learning* permettra d'automatiser l'extraction d'information dans de nombreux domaines et servira aux dirigeants les plus visionnaires.



Par exemple, dans le **secteur manufacturier**, avec le *Machine Learning*, les systèmes seront surveillés en temps réel et grâce à la détection d'anomalies, cela permettra de prévoir différents problèmes avant qu'ils ne surviennent pour ainsi maximiser la durée de vie des équipements et diminuer les interventions humaines en automatisant les processus.

En santé, le MLaaS permettra aux médecins de détecter et de diagnostiquer les maladies plus facilement grâce au logiciel *desktop doctor* qui utilise des centaines d'années de connaissances médicales.

Le MLaaS qui a passé de 480,94 M\$ en 2015 devrait atteindre 5 394,87 M\$ en 2022.

Sources:
Magazine Cloud: Big data
Statprnews