NOVEMBRE 2022 • VOL. 9 N° 10

PASSION AFFAIRES et technologies

PRÉSENTÉS CE MOIS-CI

« ARS Solutions est une entreprise qui nous guide très bien au niveau de la cybersécurité...

Nous faisons affaires avec cette firme depuis 10 ans. Leur **équipe est très compétente** et à jour dans ce monde aux avancements technologiques qui vont très vite.

Nous sommes en pleine confiance avec l'expertise de cette équipe que nous recommandons sans hésiter. »

Joannie Turcotte
VP Finances
Bois de plancher PG inc

SUIVEZ-NOUS SUR NOS RÉSEAUX SOCIAUX

- ARS Solutions Affaires-TI et Cybersécurité
- ARS Solutions Affaires et Technologies
- ARS Solutions
- arssolutions89

AFFAIRES-TI

MANQUE DE MAIN D'OEUVRE ET RÉTENTION DU PERSONNEL TI

Comment l'automatisation peut vous aider

La rétention du personnel est un enjeu de taille pour toutes les organisations, qui vivent présentement beaucoup de roulement, incluant les ressources TI. Dans un contexte de **croissance et de haute compétitivité, les entreprises ne tolèrent ni les ralentissements ni les arrêts de production**.

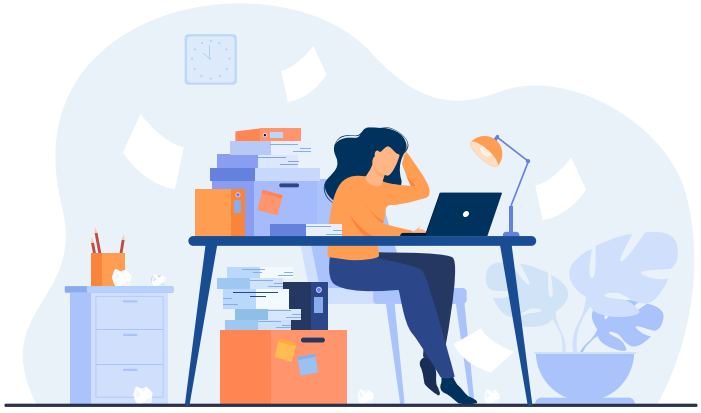
Trouver, former et garder les bonnes ressources, atténuer le roulement et ses effets, **réussir à faire le travail avec moins de personnel tout en préservant la qualité de vie des ressources...** De quoi donner bien des maux de têtes aux dirigeants, qui doivent eux aussi mettre les bouchées doubles!

SUITE PAGE 2

Principales causes de départ

Le surplus de travail, le stress et le manque d'aide sont des facteurs décisifs souvent engendrés par **l'arrivée des projets de transformation numérique** initiés par les besoins des gens qui travaillent à distance et qui utilisent plus que jamais les outils de collaboration. **Dans un contexte où les environnements informatiques sont désuets** et de plus en plus complexes – téléphonie, mobiles, tablettes – qui amène son lot d'appels quotidiens urgents.

Viennent s'ajouter le maintien des performances, de la sécurité et de la stabilité du réseau au travers les projets de mise à niveau. Une **surcharge de travail** la plupart du temps **sous-estimée**, qui fait que les ressources s'épuisent et **ne progressent pas dans leur carrière**, autre facteur important de départ. **Il devient difficile pour les supérieurs d'évaluer** la charge réelle de travail ainsi que les outils maintenant à leur disposition pour l'alléger et garder leurs ressources motivées.



L'automatisation des tâches

Une des tâches pouvant facilement être automatisée est sans aucun doute les mises à jour de sécurité des composantes réseaux. Avec de nouvelles vulnérabilités découvertes à toutes les semaines, **il est devenu impossible d'exécuter les mises à jour de sécurité manuellement sans accuser un sérieux retard et mettre l'entreprise à risque**.

Régulièrement mise de côté par manque de temps ou faite les fins de semaine, cette tâche devenue titanesque doit s'effectuer rapidement et on doit avoir l'assurance qu'elle a bien été exécutée. Longues, répétitives et ardues, **les mises à jour de sécurité sont la fondation de la sécurité** du réseau d'une entreprise et devraient être faites en-dedans de **30 jours, car les failles sont de plus en plus sévères**.

Avantages de l'automatisation

L'automatisation des mises à jour de sécurité aide votre organisation à 3 niveaux :

1. Pallier au **manque de main-d'œuvre pour une fraction du coût** d'embauche d'une ressource dédiée.

2. Favoriser la **rétention de vos ressources** TI en améliorant leur qualité de vie au travail et en allégeant leurs tâches quotidiennes pour leur permettre de se consacrer à des projets motivants et valorisants.

3. **Améliorer votre processus de cybersécurité en le rendant plus efficient** et rehausser votre posture de sécurité. **En gardant votre réseau à jour par un déploiement rapide et un meilleur contrôle de l'inventaire des équipements à risque**, vous réduisez votre fenêtre de vulnérabilité de manière significative.

L'automatisation de tâches répétitives s'avère une solution à la hauteur de la conjoncture actuelle dont le but est d'aider les entreprises à faire face au manque de main-d'œuvre et à la compétition, deux enjeux majeurs.

AUTOMATISATION DES MISES À JOUR DE SÉCURITÉ

La solution au manque de main-d'oeuvre et à la rétention du personnel TI

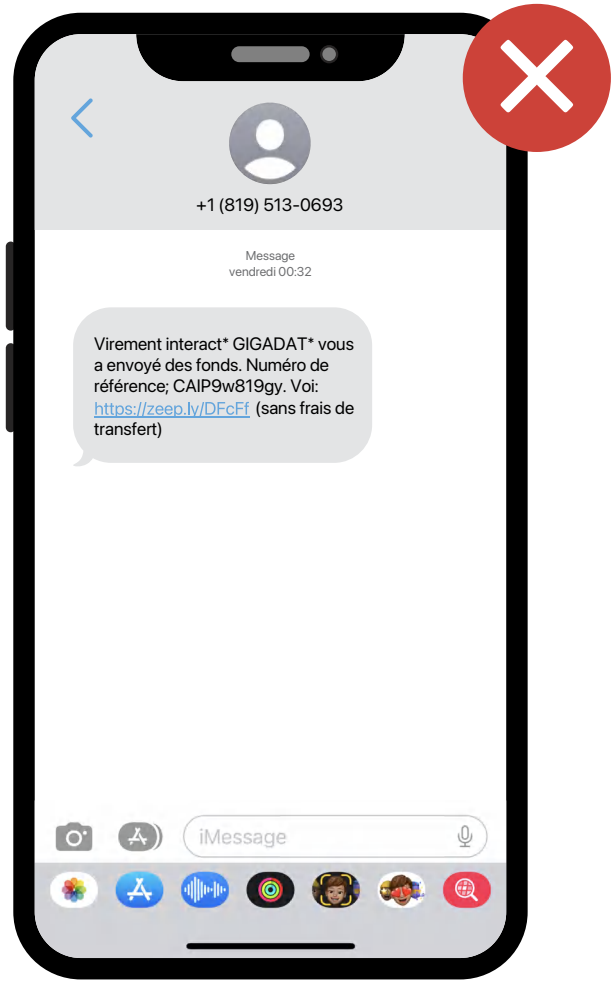
Découvrez les 3 principaux avantages d'automatiser :
www.ars-solutions.ca/retention/

2B UPDATED

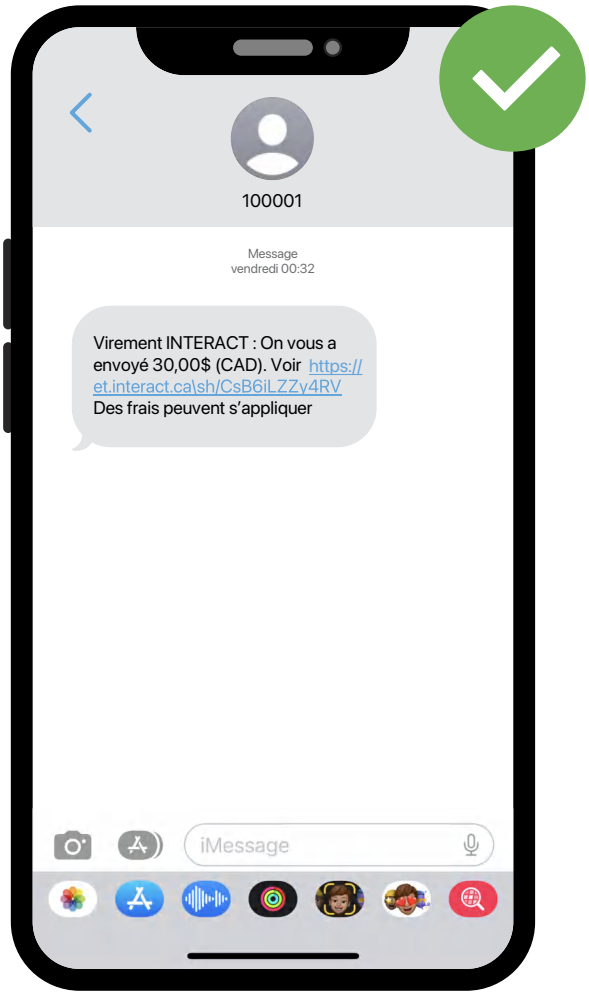
MÉFIEZ-VOUS DES VIREMENTS INTERACT

Le *Virement Interac* est de plus en plus populaire pour déposer automatiquement des fonds directement dans votre compte bancaire, sans mot de passe à retenir ou erreur de frappe, via votre numéro de téléphone cellulaire ou votre adresse courriel.

Cette technique est plus rapide et moins complexe que les virements bancaires, mais elle est malheureusement vite tombée dans la mire des cybercriminels. Avec un emploi du temps très chargé, il est parfois facile d'oublier qu'une personne ou une société vous doit de l'argent, et les malfaiteurs le savent. Ce pour quoi ils vont envoyer des campagnes d'hameçonnage de masse par courriel ou texto ressemblant à celui-ci :



Attention : l'image précédente représente une tentative d'hameçonnage de *Virement Interac* par texto. Il provient **d'un numéro de téléphone inconnu et le message est différent de l'exemple légitime ci-dessous** provenant d'une véritable banque identifiée au numéro générique "100001" avec un lien du service *Interac*. Les deux sont toutefois très semblables donc il est **facile de s'y méprendre et de tomber dans le panneau**.



Quoi faire?

100001 est l'adresse de code court d'où proviennent toutes les notifications de *Virement Interac* par texto. Ne cliquez que sur les liens des notifications *Interac* provenant d'expéditeurs que vous connaissez et de demandes que vous attendiez. Si vous ne vous attendiez pas à ce que ce contact vous envoie des fonds, signalez-le. Vous pouvez **signaler un courriel/texto** en appelant le Centre de services aux membres d'*Interac* ou en envoyant un courriel à **phishing@interac.ca**. N'hésitez pas à communiquer avec nous si vous avez besoin d'aide à ce sujet.

3 ÉTAPES
POUR BLOQUER LES COURRIELS SPAM

Vous êtes tanné de voir votre boîte courriel inondée par des spams?
Voici comment les bloquer et nettoyer votre boîte de réception pour de bon.

Selon les données de Statista, les spams représentaient près de **50 % du trafic de courrier électronique en septembre 2020**. Sur les **293,6 milliards de courriels envoyés quotidiennement en 2019**, la majorité étaient des courriels promotionnels provenant de spécialistes du marketing. Mais tous les courriels dans votre boîte de réception ne sont pas des publicités inoffensives. Certains pourraient mettre votre appareil et votre sécurité en danger, affirment les experts.

Pourquoi je reçois ces courriels?

Il est courant de recevoir des messages d'hameçonnage et des courriers indésirables lorsque vous donnez votre adresse électronique à des sites Web douteux, par exemple en remplissant des formulaires pour des publicités promettant des "trucs gratuits". Les cybercriminels peuvent voler votre adresse électronique en usurpant les services et organisations légitimes avec lesquels vous l'avez partagée, puis vendre ces informations à des malfaiteurs qui espèrent vous escroquer. Les entreprises et les annonceurs partagent également des listes de contacts publiques pour envoyer des courriels de marketing de masse. Heureusement, la plupart des fournisseurs de messagerie - dont Gmail, iPhone, Outlook, Yahoo, Hotmail et AOL - permettent aux utilisateurs de bloquer les spams et les courriers indésirables sur leurs plateformes. Suivez ce guide étape par étape pour bloquer les courriels de spam avec chaque serveur de messagerie.

Comment bloquer les courriels sur Gmail

Navigateur Web
1. Ouvrez un courriel de l'expéditeur que vous souhaitez bloquer
2. Cliquez sur l'icône à trois points "Plus" dans le coin supérieur droit
3. Cliquez sur "Bloquer"

Application
1. Ouvrez un courriel de l'expéditeur que vous souhaitez bloquer
2. Appuyez sur l'icône à trois points "Plus" dans le coin supérieur droit
3. Sélectionnez "Bloquer l'expéditeur"

Comment bloquer les courriels sur l'iPhone
1. Ouvrez l'application Mail
2. Ouvrez un courriel de l'expéditeur que vous souhaitez bloquer
3. Touchez le nom de l'expéditeur
4. Touchez l'adresse indiquée à côté de "De" dans l'en-tête
5. Choisissez "Bloquer ce contact"
6. Confirmez que vous voulez bloquer le contact

Comment bloquer les courriels sur Outlook

Navigateur Web
1. Ouvrez un courriel de l'expéditeur que vous voulez bloquer
2. Cliquez sur les trois points horizontaux dans le coin supérieur droit
3. Sélectionnez "Bloquer"

Application
1. Ouvrez un courriel de l'expéditeur que vous souhaitez bloquer
2. Tapez sur l'icône à trois points dans le coin supérieur droit
3. Sélectionnez "Déplacer vers Spam"

Bureau
1. Cliquez avec le bouton droit de la souris sur le courriel de l'expéditeur que vous souhaitez bloquer
2. Cliquez sur "Courrier indésirable" > "Bloquer l'expéditeur"

Comment bloquer les courriels sur Yahoo

Navigateur Web
1. Ouvrez un courriel de l'expéditeur que vous souhaitez bloquer
2. Cliquez sur l'icône à trois points en haut du courriel
3. Cliquez sur "Bloquer l'expéditeur"

Application
1. Appuyez sur le menu dans le coin supérieur gauche
2. Choisissez "Outils" > "Filtres"
3. Appuyez sur l'icône "+" dans le coin supérieur droit
4. Choisissez un nom pour le nouveau filtre
5. Tapez l'adresse électronique que vous voulez bloquer dans le champ "Expéditeur"

Comment bloquer les courriels sur Hotmail

1. Cliquez sur "Accueil" > "Paramètres" > "Afficher tous les paramètres d'Outlook"
2. Cliquez sur "Email" > "Courrier indésirable" > "Filtres"
3. Tapez le nom de l'expéditeur sous "Expéditeurs bloqués"

Comment bloquer les courriels sur AOL

1. Sous votre nom d'utilisateur, cliquez sur "Options/Paramètres de messagerie"
2. Cliquez sur l'onglet "Expéditeurs bloqués"
3. Saisissez l'adresse électronique que vous souhaitez bloquer
4. Cliquez sur l'icône "+"
5. Sélectionnez "Enregistrer les paramètres"

Que faire si vous recevez un courriel suspect?

Ignorer les courriels suspects est le moyen le plus sûr de se protéger contre les cybercriminels et les voleurs. « Tant que vous ne cliquez pas sur des liens inconnus ou non sollicités, sur des pièces jointes ou que vous ne téléchargez pas de fichier, vous aurez fait à peu près tout ce que vous pouvez faire pour éviter toute attaque contre votre ordinateur ou vos données », explique James E. Lee, chef des opérations de l'Identity Theft Resource Center. Si vous recevez un courrier électronique d'une personne de confiance, mais que vous n'êtes pas sûr du lien ou de la pièce jointe, contactez votre partenaire TI pour valider sa légitimité. Et avant de répondre au courriel, faites attention aux signes qui indiquent que vous êtes sur le point de tomber dans une arnaque d'hameçonnage.

Comment éviter de recevoir des spams ou des courriels non désirés?

Si vous en recevez beaucoup, prenez un nouveau départ avec deux nouveaux comptes de messagerie : un pour les opérations marketing et un autre pour les courriels privés avec les amis et la famille. Une fois que vous avez vos nouvelles adresses, il faut limiter avec qui et quand vous les partagez. « Vous ne devez partager vos informations personnelles qu'avec des organisations de confiance et uniquement lorsque c'est nécessaire », indique M. Lee. Il suggère également de protéger vos comptes avec des outils de confidentialité comme l'authentification multifactorielle (MFA), si possible, pour ainsi garder une longueur d'avance sur les cybercriminels.

Source : Brooke Nelson