Cism Gestion Informatique

Le Journal TECHNO

Août 2021

Quoi de neuf ?

NOUVEAUTÉ

Suite aux avancés des technologies Cloud & de « Téléphonie IP », à toute la publicité entourant ces solutions, et aux préoccupations d'entrepreneurs de Montréal concernant les factures téléphoniques onéreuses : nous avons préparé, **pour vous**, un **Guide utile & complet** pour vous aider dans votre prise de décision *(voir à la page 2).*

Après lecture, si vous êtes encore indécis ou embêté et que vous ne voulez pas commettre une erreur coûteuse, alors notre **Évaluation Gratuite de vos communications** vous fournira les **informations privilégiées** dont vous avez besoin pour votre PME. Appelez-moi au **514-830-8184 (101)** ou inscrivez-vous au www.cisminformatique.com/phone-assessment/.

Il n'y a aucune attente de ma part, sauf de vous aider à faire le meilleur choix pour amener votre PME à un niveau supérieur.

Août 2021

Cette publication mensuelle est une gracieuseté de Bernard Houde, Président de CISM Gestion Informatique.

Notre Mission est de vous aider à réaliser vos projets de croissance grâce à nos solutions innovantes en matière de Serveurs, de Logiciels, de Cloud, de Sécurité, de Maintenance et de Surveillance en temps réel. Nos mots d'ordre sont **Efficacité**, **Fiabilité** et **Sécurité**.

Vagues de Chaleur Extrême ! Comment les Canicules Peuvent Faire des Ravages sur Votre Technologie

Au Québec, les jours de canicule sont là de plus en plus tôt l'été, et il fait très chaud dehors ! Les propriétaires de maison et les propriétaires d'entreprise se préparent à leurs prochaines factures d'électricité alors qu'ils font fonctionner leurs climatiseurs 24 heures sur 24 en essayant de rester au frais. Mais pour de nombreux propriétaires d'entreprise, il ne s'agit pas seulement de garder votre équipe au frais, il s'agit également de garder votre technologie au frais.

Chaque pièce de technologie que vous utilisez est susceptible d'être endommagée par la chaleur. Parfois, ils surchauffent en raison de problèmes internes. Peut-être qu'ils traitent beaucoup de données. Ou peut-être que le système de refroidissement interne ne suffit pas. Mais ils peuvent également surchauffer en raison de problèmes externes, tels que des températures estivales élevées et une climatisation inadéquate.

Si la chaleur submerge vos systèmes, elle a le potentiel d'assommer votre entreprise. Si les ordinateurs tombent en panne ou que les serveurs ne peuvent pas fonctionner efficacement en raison de la chaleur, cela peut être un désastre coûteux. L'ordinateur moyen est conçu pour fonctionner à des températures externes de 10 à 28 degrés Celsius. Les ordinateurs portables et les tablettes peuvent supporter de 10 à 35 degrés Celsius.

Chaque entreprise doit être consciente des dommages que la chaleur peut causer. Par exemple, la chaleur peut endommager les composants individuels de vos appareils. Il existe des enregistrements de cartes graphiques prenant feu à la suite de surchauffe et de problèmes électriques liés à la chaleur. Ces composants sont conçus pour résister à une chaleur élevée, mais ils ne peuvent en supporter qu'une certaine quantité.

La chaleur peut également perturber la productivité. C'est une chose si

Suite à la page 2

Suite de la page 1

votre entreprise est plus chaude que d'habitude et que vous avez des fans en marche. Cela peut rendre le travail plus difficile. Mais la chaleur ralentit les appareils. Ils ne peuvent pas fonctionner aussi efficacement et, par conséquent, les programmes et les applications auront du mal à fonctionner. Dans certains cas, ils peuvent ne pas être en mesure de fonctionner du tout car ils nécessitent une certaine quantité de traitement de données qui est négativement affectée par une trop grande chaleur.

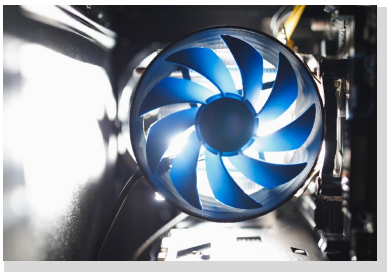
Si vos systèmes sont perturbés ou endommagés, vous pouvez également perdre des données critiques. La chaleur peut endommager les disques durs et les disques SSD, vous laissant sans accès à vos données. Parfois, avec un refroidissement approprié, ces données peuvent être récupérées, mais si la chaleur et les dommages persistent, les données peuvent être irrécupérables si vous n'avez pas de sauvegarde.

Quelle est la prochaine étape ? Chaque entreprise doit bien comprendre ses besoins en refroidissement. C'est une chose de refroidir les gens qui travaillent dans un bureau. C'est tout autre chose de refroidir une salle de serveurs. Posez-vous donc des questions comme :

• Mon entreprise dispose-t-elle d'une climatisation adéquate et efficace ?

> **"Chaque pièce de technologie que vous utilisez peut être endommagé par la chaleur."**

• Notre technologie (salle informatique ou serveurs) dispose-t-elle d'une climatisation adéquate ?



• Nos appareils individuels ont-ils un refroidissement adéquat (les employés se sont-ils plaints de ralentissements étranges des applications) ?

En plus de cela, il est essentiel de vous poser des questions sur vos besoins en matière de sécurité des données :

• Conservons-nous toutes nos données sur place ?

• Nos données sont-elles protégées contre les catastrophes ou les intrusions extérieures (avons-nous investi dans la cybersécurité) ?

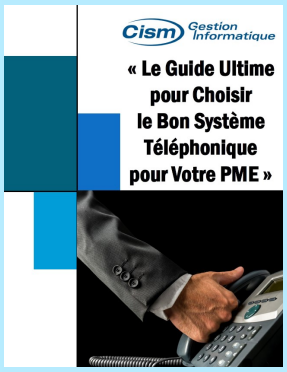
• Avons-nous un plan si nos données sont endommagées ou perdues ?

• Sauvegardons-nous régulièrement nos données dans le cloud ou une autre solution hors site ?

Vous n'avez jamais à compromettre vos données ou votre entreprise. Il existe aujourd'hui **d'innombrables solutions** sur le marché pour vous aider à **protéger vos actifs les plus précieux** et pour répondre à vos besoins de refroidissement technologique. Lorsque les canicules de l'été s'installent et persistent, n'oubliez pas que vous avez des options. Un fournisseur de Services gérés (MSP) ou une société de Services informatiques expérimentée peut vous aider à déterminer si votre technologie est aussi « excellente » qu'elle devrait l'être. Ils peuvent vous aider à assurer la longévité de votre technologie et à protéger vos données.

Télécharger notre Rapport GRATUIT : « Le Guide pour choisir le meilleur Système Téléphonique pour Votre PME »

Lisez-le pour découvrir :



- Qu'est-ce que la **VoIP**, **comment ça fonctionne** & pourquoi une compagnie de téléphones peut vous forcer à passer à la Téléphonie IP dans les 2-3 années à venir ;
- **4 façons** différentes **d'implémenter la VoIP** et pourquoi vous ne devriez jamais en utiliser 3 pour un Système téléphonique d'entreprise ;
- Des **coûts cachés** avec certains systèmes VoIP qui peuvent **annuler** toutes les **économies** que vous pourriez réaliser sur votre facture de téléphone ;
- **24 questions** révélatrices à poser à n'importe quel vendeur VoIP pour **voir clair** à travers les demi-vérités qu'ils vous diront pour conclure la vente ;
- **Liste de contrôle** pour comparer les vendeurs de Systèmes Téléphoniques de qualité professionnelle (**quoi rechercher** comme système & service ?).

Demandez votre guide GRATUIT dès aujourd'hui sur: https://www.cisminformatique.com/phoneguide/

Pleins feux sur nos précieux clients

C'est en 1991 que la PME a débuté sous le nom de Centre du Camion Serafin Volvo. Un trio familial s'est alors formé, jumelant connaissance mécanique, sens de l'administration et du service à la clientèle, avec une expertise en bâtissage, réparation de transmissions & de différentiels de véhicules lourds comme : camions routiers & de transport et engins de chantiers. Au fil des ans, la PME s'est distinguée par sa capacité de s'adapter à divers marchés.

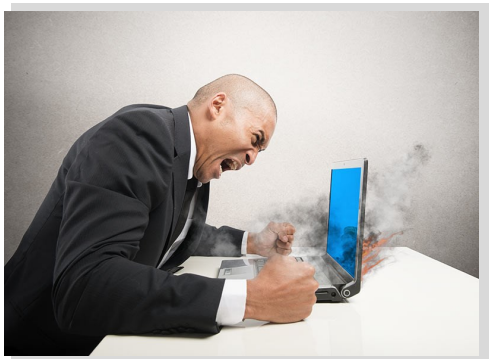
En 2015, elle est devenue **Solutions Serafin Inc.** pour refléter une image plus fidèle de leur mission : un **Centre de services** ayant pour but d'offrir des **solutions de qualité, avantageuses et sur mesure** pour leurs clients. Ils ont créé des relations corporatives avec des partenaires comme le Port de Montréal et d'Halifax, des sociétés de transport public et bien plus.

Aujourd'hui, la 3e génération des Serafin poursuit fièrement avec passion, innovation & partage de leurs connaissances, tout en élargissant leur réseau d'approvisionnement & en ayant à cœur la clientèle avec laquelle elle grandit chaque jour. Elle offre à son personnel de la formation & des solutions informatiques adaptées avec l'aide de CISM Gestion Informatique.

«CISM est une équipe de professionnels donnant un excellent service, rapide, clairs dans leurs réponses, avec des solutions adaptés à nos besoins et **nous offrant la tranquillité d'esprit que notre entreprise recherche**. »

Solutions Serafin inc. fait confiance à CISM pour la gestion & la sécurité de l'ensemble de son parc informatique

Prudence avec les courriels



4 types de courriels que vous ne devriez jamais ouvrir. Peu importe comment votre réseau est « à l'épreuve » des malveillants, vous et vos employés pouvez toujours inviter un pirate, si vous cliquez sur un lien ou ouvrez une pièce jointe d'un courriel envoyé par un cybercriminel. Certains pourriels sont évidents (pouvez-vous dire, « Viagra à rabais »?), mais d'autres sont très habilement conçus pour se faufiler devant tous les filtres et tromper le destinataire en ouvrant la porte. Connu sous le nom de « courriel d'hameçonnage », c'est toujours la **façon #1** dont les pirates contournent les pare-feu, filtres et antivirus, il est donc important que vous et vos employés sachiez comment repérer un courriel menaçant. Voici 4 types de stratagèmes de courriel pour lesquels vous devriez être en état d'alerte.

Le courriel de demande urgente. Le plus courant courriel d'hameçonnage est celui qui usurpe l'identité de votre banque, du gouvernement ou d'une figure d'autorité. La règle d'or est la suivante, tout courriel dont : **1)** vous ne connaissez pas personnellement l'expéditeur, y compris les courriels du gouvernement, Microsoft ou votre « banque », et **2)** vous demande de « vérifier » votre compte doit être supprimé immédiatement. N'oubliez pas que toute notification importante sera envoyée par courrier postal à l'ancienne. Aussi, si c'est important, ils peuvent vous appeler.

Le courriel de « Vérification de compte ». Tout courriel vous demandant de vérifier votre mot de passe, vos informations bancaires ou d'identification de connexion, ou de mettre à jour les informations de votre compte, doit être ignoré. Aucun fournisseur légitime n'envoie de courriels demandant cela; ils vous demanderont simplement de vous connecter pour mettre à jour ou vérifier vos informations si cela est nécessaire.

Le courriel avec des fautes de frappe. Un autre grand signe avant-coureur est la faute de frappe. Les courriels provenant de l'étranger (d'où proviennent la plupart de ces attaques) sont écrits par des personnes qui ne parlent pas ou n'écrivent pas bien le français. Par conséquent, s'il y a des fautes de frappe évidentes ou des erreurs de grammaire, supprimez-le.

Le fichier Zip, pdf ou pièce jointe de facture. Sauf si vous connaissez spécifiquement l'expéditeur d'un courriel, jamais, ne jamais ouvrir une pièce jointe. Cela inclut les fichiers PDF, les fichiers zip, les fichiers musicaux et vidéo et tout ce qui fait référence à une facture impayée ou un fichier comptable (de nombreux pirates utilisent cela pour amener les gens des départements comptables à ouvrir ces courriels). Bien sûr, n'importe quel fichier peut transporter un virus, donc mieux vaut le supprimer que d'être désolé.

Par **Bernard Houde**, Président et conseiller senior, **CISM Gestion Informatique**

Voici comment la technologie renforce le lieu de travail

Dans le passé, beaucoup d'entre nous étaient convaincus que le travail sur place (au bureau) était le modèle idéal pour favoriser la culture d'entreprise et maximiser la collaboration. Bien que cela soit vrai, considérant le monde « post-pandémique », nous avons appris que nous pouvons développer la culture d'entreprise et une collaboration solide, même avec les lieux de travail numériques.

Apprendre cela n'a pas été facile, cela a nécessité beaucoup d'essais et d'erreurs. Cependant, les environnements de travail à distance ont ouvert de nouvelles portes et permis aux entreprises d'essayer des technologies qu'elles auraient peut-être manquées ou ignorées avant. Ces technologies incluent des logiciels de gestion de projet, des outils de communication et même des calendriers avancés qui permettent aux employés – à distance et en personne – de vraiment planifier leurs journées.

Cela a également incité les entreprises à **repenser la cybersécurité**. Au fur et à mesure que de plus en plus de propriétaires sont devenus distants, ils ont dû trouver comment assurer la sécurité de leur entreprise et de leurs employés. Dans le passé, ils ont peut-être échoué dans le domaine de la cybersécurité, mais maintenant, ce n'est plus le cas. En adoptant de nouvelles technologies et idées, ils ont fini par renforcer leurs entreprises pour un avenir différent.
Inc., 13 avril 2021

Une approche différente pour renforcer vos revenus

Steven Knight, entrepreneur et contributeur de Forbes, partage son approche pour renforcer les revenus et la santé d'une entreprise. En tant que créateur de solutions et d'opportunités chez Mosaic Home Services Ltd., il offre une vision approfondie du sujet.

Malgré que ce soit un sujet important, il se concentre sur le « client ». Chaque propriétaire d'entreprise doit se demander : « Qui voulez-vous que votre client soit ? » Il s'agit d'essayer de vraiment comprendre qui devrait ou doit être votre client idéal. Évitez de faire des suppositions sur vos clients et sur les personnes que vous pensez devoir cibler.

Cela revient à regarder votre expertise. Il est tentant d'offrir des services vaguement liés à ce que vous faites déjà afin de cibler de nouveaux clients, mais vous devez vous demander si cela en vaut la peine. Au lieu de cela, doublez les clients que vous servez déjà et servez-les bien, puis cherchez-en plus. Ce n'est pas facile, mais pour renforcer vos revenus, vous devez déterminer qui et ce qui compte vraiment.
Forbes, le 17 mai 2021

4 cyber-défis à suivre dans votre radar

Attaques d'infrastructures. Celles-ci sont en augmentation et ont le pouvoir de perturber les chaînes d'approvisionnement, comme les Américains l'ont appris avec les pénuries de gaz aux États-Unis en mai. Verizon rapporte qu'une majorité (environ 71%) des attaques consistent à extorquer de l'argent. L'attaque du pipeline était une attaque de rançongiciel.

Plus grande persistance. Avec davantage de personnes travaillant à distance, plus d'entreprises s'appuyant sur l'intelligence artificielle et l'automatisation, et plus d'appareils connectés, les cybercriminels recherchent de nouvelles façons d'exploiter tous ces domaines.

Les cybercriminels travaillent ensemble. Aussi étrange que cela puisse paraître, de nombreux cybercriminels travaillent davantage ensemble que par le passé. Ils s'appuient sur des marchés noirs et des forums cachés où ils peuvent acheter les derniers outils perturbateurs et discuter de tactiques.

L'Internet des objets. Il existe d'innombrables appareils qui font partie de l'Internet des objets, notamment des thermostats, des réfrigérateurs, et même, des défibrillateurs. Ces appareils peuvent être difficiles à protéger des intrusions extérieures et les utilisateurs doivent être conscients de la sécurité présente sur ces appareils et éviter ceux qui en sont privés.
Forbes, le 9 mai 2021

"This is the third cheese delivery this month. Not only do we have mice, they appear to be tech savvy."