Cism Gestion Informatique

Le Journal TECHNO

Juin 2022

Nouveautés et Tendances

L'une des 12 tendances technologiques et stratégiques identifiée par Gartner pour 2022 :

L'Entreprise Distribuée

Si elle est loin d'être la norme, elle s'est accentuée avec la crise sanitaire. Selon Gartner, cette approche privilégie le **VIRTUEL** et le **DISTANT**, elle peut aussi être appliquée aux clients et prospects d'une entreprise, afin d'offrir une expérience davantage digitalisée et adaptée aux nouveaux modes de travail et de consommation.

D'ici 2023, les 3/4 des entreprises qui opteront pour cette tendance verront leurs revenus croître de 25% plus rapidement que leurs concurrents. Pour en apprendre davantage sur **nos stratégies** & **solutions** à ce sujet, communiquez sans tarder avec Bernard au **(514) 830-8184** (101#).

Juin 2022

Publication mensuelle de **Bernard Houde,** Président **CISM Gestion Informatique**

Pourquoi La "Génération Z" Pourrait Constituer Une Menace Pour La Sécurité De Votre Entreprise ?

Et comment se préparer ?

Au fur et à mesure que nous progressons jusqu'en 2022, de plus en plus de personnes de la **Génération Z** entreront sur le marché du travail. Lorsque les milléniaux sont entrés sur le marché du travail, nous avons vu des attitudes et des comportements différents que jamais auparavant, et nous devrions nous attendre à ce que les membres de la **Génération Z** viennent avec leur propre unicité et leurs différences. Vous pensez peut-être que puisqu'ils sont la 1ère génération complète à grandir à l'ère numérique, ils seront bien préparés pour tous les défis technologiques et les problèmes de sécurité qui se posent, mais ce n'est pas toujours le cas.

Étant donné que la plupart des gens de la **Génération Z** ont grandi avec un téléphone intelligent et les médias sociaux, ils sont plus susceptibles de partager des informations sans aucun souci de sécurité. Selon des Entrepreneurs, de nombreux membres de la **Génération Z** ont du mal à faire la distinction entre les amis qu'ils ont rencontrés en ligne et dans la vraie vie. Les cybercriminels pourraient utiliser ces connaissances pour créer avec soin des profils de médias sociaux afin d'accéder à des informations précieuses sur l'individu et peut-être même sur son lieu de travail.

Il existe de nombreux problèmes communs qui affligent la **Génération Z** en matière de cybersécurité. Les problèmes de mot de passe semblent être les plus répandus. Selon un récent sondage Harris, 78 % des membres de la **Génération Z** utilisent le même mot de passe sur plusieurs comptes. C'est une augmentation de 10 à 20 % par rapport à la **Génération Y**, à la **Génération X** et aux **baby-boomers**. Les autres problèmes courants sont les habitudes de navigation sécurisées sur les réseaux sociaux et l'internet.

Au cours des prochaines années, il y a de fortes chances que vous embauchiez un « **Gen Zer** » pour un rôle dans votre entreprise. Vous vous demandez probablement comment vous pouvez préparer votre cybersécurité pour qu'elle soit prête à gérer tout ce que la prochaine génération apportera. Il est important que vous soyez proactif dans votre stratégie. Attendre d'avoir déjà des gens de la **Génération Z** sur votre lieu de travail pourrait laisser vos informations sans protection ou rendre votre entreprise vulnérable aux cyberattaques.

Suite à la page 2

Suite de la page 1

Avant toute chose, vous devez développer un programme de formation en sécurité de l'information. Il est impératif que votre entreprise ait une culture de cybersécurité bien établie à laquelle tout le monde adhère. De cette façon, lorsque vous avez de nouvelles recrues, vous pouvez leur faire suivre la même formation pendant que vos autres employés démontrent les bonnes techniques par leur comportement. Assurez-vous que votre formation est à jour et que vous continuez à la mettre à jour chaque fois qu'un nouveau logiciel ou une nouvelle technologie est publiée.

Souvenez-vous quand nous avons mentionné que plusieurs de la **Génération Z** ont du mal avec la sécurité des mots de passe et utilisent souvent le même mot de passe pour chaque compte ? S'ils continuent à le faire et à utiliser le même mot de passe pour leurs comptes personnels et professionnels, cela pourrait rendre votre entreprise vulnérable. Commencez à mettre en œuvre des programmes de gestion de mots de passe dans votre entreprise dès que possible pour éviter ce dilemme avec les employés actuels ou futurs. Les gestionnaires de mots de passe créent des mots de passe plus compliqués et sécurisés qu'un pirate informatique moyen ne peut pas déchiffrer.

Si vous voulez vraiment protéger votre entreprise contre les cybercriminels, vous pouvez faire appel à un Fournisseur de Services Gérés (MSP) pour répondre à vos besoins informatiques. Ils sont avant tout proactifs, avec eux, vous bénéficierez d'une surveillance 24h/24, du cryptage & de la sauvegarde de données, de la protection du réseau & du pare-feu, d'une formation de sensibilisation à la sécurité et bien plus. Fondamentalement, toutes vos préoccupations en matière de cybersécurité seront couvertes lorsque vous embaucherez un MSP, et vous n'aurez même pas à vous soucier de la prochaine génération qui rendra les choses plus difficiles.

> **" 78% des "Gen Zers" utilisent le même mot de passe sur plusieurs comptes."**

Alors que la **Génération Z** entre sur le marché du travail, il est important que tous les propriétaires d'entreprise se préparent à leur arrivée. N'attendez pas qu'ils commencent dans votre entreprise pour apporter des modifications à votre « Plan de cybersécurité ». Soyez proactif et faites ce qu'il faut pour vous assurer que votre entreprise est parfaitement préparée. Sachez que **CISM Gestion Informatique** détient l'expertise et les solutions pour que vous soyez prêt à accueillir cette nouvelle génération d'employés. Communiquer simplement avec Bernard au **514-830-8184** (101#).

Québec

Offensive de transformation numérique - Plus de 29 M$ pour accélérer le virage numérique d'entreprises partout au Québec

Si vous n'avez pas encore pris connaissance de cette nouvelle du 20/04/2022 concernant l'attribution d'aides financières du Gouvernement du Québec, cliquez sur le lien suivant pour lire le texte : https://www.quebec.ca/nouvelles/actualites/details/offensive-de-transformation-numerique-plus-de-29-m-pour-accelerer-le-virage-numerique-dentreprises-partout-au-quebec-39538

Choisirez-vous notre SÉCURITÉ 3.0 ?

La SÉCURITÉ est un enjeu d'affaires continu, CISM a développé pour les PME une Solution Avancée Complète couvrant l'ensembles de leurs besoins.

Solution Avancée de Sécurité, la Sécutié 3.0

Notre protection de plus en plus réclamée !

C) Protection Infonuagique :

- 0365 Backup & Politiques de sécurité
(sauvegarde d'0365 4 fois par jour (courriel, OneDrive, SharePoint, TEAMS) + gestion des politiques de sécurité de la plateforme 0365)
- Anti pourriel
(filtrage antipourriel pour les courriels reçus et envoyés)

Inscrivez-vous Gratuitement à notre Audit CyberSécurité au :
cisminformatique.com/guides-gratuits/

Pleins feux sur nos précieux clients

La firme **Yves Woodrough Architectes inc.** (**YWA**) est un « cabinet boutique » spécialisé en architecture institutionnelle, innovateur et avant-gardiste. Le cabinet offre une expérience de projet axée sur l'écoute, la consultation et le respect de ses clients.

Leur expertise et leur expérience reconnue depuis plus de 40 ans, leur permettent d'intervenir avec succès dans des établissements institutionnels : de santé & services sociaux, d'enseignement & éducation, municipaux et autres.

Le cabinet boutique s'occupe de ses clients de façon conviviale, en toute simplicité et avec une grande disponibilité. Celui-ci innove grâce à une prestation de services directs et flexibles, de plus, ses associés sont impliqués personnellement dans le développement de tous les projets. Sa clientèle se situe principalement à Montréal et sur la Rive Nord. La firme a réalisé des projets de tous les types ainsi que de toutes les envergures : nouvelle construction, agrandissement, rénovation fonctionnelle ou réparation.

YWA fait confiance à **CISM** pour ses **Services Informatiques**.

Soyez « Cyber Smart »

(#BeCyberSmart)

Nos Meilleurs Conseils de Sécurité du Mois

CONSEIL #2 - Vous travaillez à domicile, FAITES ATTENTION !

Étant donné que vos employés peuvent être tenus de travailler à domicile, leur état d'esprit peut être : « *Je peux aussi bien utiliser mon ordinateur personnel* ». Sachez que c'est une erreur dangereuse.

Les ordinateurs personnels et les appareils mobiles personnels pourraient être jonchés de tonnes de musique, vidéos, images téléchargées, etc. Parce qu'il est plus exposé, il peut inviter des logiciels malveillants dans votre réseau d'entreprise.

SEULS les appareils qui sont sous notre surveillance vigilante en matière de correctifs et mises à jour doivent être utilisés par vos employés pour travailler à distance. Fournissez un ordinateur sécurisé et approuvé par l'entreprise pour que les employés puissent l'utiliser à la maison.

CONSEIL #3 - Améliorez votre stratégie de mot de passe

En cas de crise mondiale comme une pandémie ou catastrophes à grande échelle, vos mots de passe peuvent faire la différence entre passer votre temps à essayer de récupérer des finances et des données privées qui ont été piratées..

Mesures à prendre pour protéger vos mots de passe :

1. Passez en revue vos mots de passe actuels et informez votre équipe pour en créer des plus forts et plus complexes qui ne peuvent pas être facilement devinés.
2. Utilisez un logiciel de gestion de mots de passe pour stocker tous vos mots de passe au même endroit. Ne les stockez pas dans votre navigateur Web simplement parce que c'est pratique. C'est aussi facile à pirater.

Vous avez besoin de conseils pour sécuriser vos télétravailleurs ? Réservez votre rencontre virtuelle de 15 minutes via mon agenda au << http://go.scheduleyou.in/vryhFk >>. Pour tout autre besoin informatique urgent, joignez-moi au **514-830-8184** (101#).

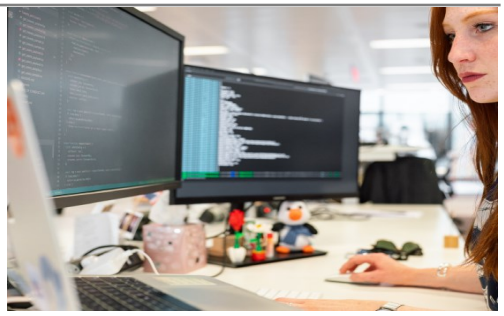
Bernard Houde
Président et Expert-Conseil

*Je suis **Bernard Houde**, passionné de protéger & éduquer les gens en **CyberSécurité**. Depuis plus de 24 ans, nous gèrons les Systèmes informatiques de nos clients à distance, des **PME** de la région de **Montréal** comptant de **10 à 100 ordinateurs.** Je parle à des MSPs & dirigeants d'entreprises régulièrement. Si vous êtes **préoccupé par la sécurité de votre PME** ? Vous voulez certainement **être aidé par des Experts maîtrisant les dernières technologies**. Je suis disponible pour répondre à toutes vos questions.*

Bonne Pratique Informatique d'Entreprise

(Sécurité Physique)

9. Éteignez votre ordinateur quand vous quittez le bureau. Cela prolongera sa durée de vie, et au démarrage, il sera plus performant et exempt de corruption et/ou de saturation de la mémoire vive.



Trucs et Astuces pour gagner en efficacité

Gestion des témoins (cookies)

Un **témoin** ou un « **cookie** » est un petit fichier texte qu'un serveur web installe sur l'ordinateur d'un internaute lors de sa visite sur un site web. Ce fichier peut être récupéré par ce serveur lors de visites subséquentes. (Source : Glossaire informatique)

Un témoin est très utile, il sert à authentifier (identifiant & mot de passe d'un site), à maintenir l'état d'une session ou à conserver une information spécifique de l'internaute (informations du profil, préférences de site, références de facturation, contenu du panier d'achat électronique). ***Les témoins ne sont ni des logiciels espions, ni des virus.***

Acceptation ou refus des témoins : Par défaut, les navigateurs sont configurés pour accepter les témoins. En modifiant les préférences, vous pouvez refuser les témoins ou vous faire alerter lorsqu'un site tente d'en implanter un, permettant l'acceptation ou le refus d'un témoin spécifique.

Suppression des témoins : La plupart des témoins sont conservés le temps d'une session & automatiquement supprimés du disque dur à la fermeture de la session ou du navigateur. Pour les témoins dont la durée de conservation est plus longue, il peut être judicieux de conserver ceux des sites souvent visités et ceux servant à la reconnaissance & à l'identification lors du retour sur un site (évitant la saisie à nouveau de renseignements d'identification).

Gestion des témoins selon le navigateur

Google Chrome

- Cliquer sur le menu Google Chrome ou , puis choisir **Paramètres**
- Dans la page qui s'ouvre, cliquer sur le sous-menu
  Confidentialité et sécurité
- Dans le menu apparaissant à droite, cliquer sur
  Cookies et autres données des sites
  Les cookies sont autorisés
- À la rubrique **Paramètres généraux**, choisir la façon dont les témoins seront gérés (Autoriser, Interdire avec les différentes options de Blocage, Conserver pour la session, , etc.)
- Pour effacer des témoins, cliquer sur **Afficher l'ensemble des cookies et données de sites**, puis cliquer sur le bouton **Tout supprimer** pour effacer tous les témoins d'un coup, ou bien, cliquer sur les noms de domaine pour supprimer les témoins individuellement (à l'aide du **X**).

Saviez-vous que …

Microsoft ne prend pas en charge vos sauvegardes de courriels et de données ? Et que la conservation & la sauvegarde de vos données de la plateforme d'Office 365 sont de VOTRE RESPONSABILITÉ.

Même si l'environnement vous permet d'opérer votre transformation numérique, Microsoft invite à la prudence et recommande des sauvegardes complètes. Créez, connectez-vous et partagez où que vous soyez avec : l'intranet mobile & intelligent **SharePoint**, l'espace de stockage en ligne **OneDrive**, le courrier & calendrier **Outlook**, le bloc-notes numérique **OneNote**, le travail d'équipe dynamique **Teams**, et bien plus encore.

Il est important de sauvegarder vos courriels et données d'**Office 365**, 4 fois par jour (à chaque 6 heures). Sachez que les experts de CISM Gestion Informatique peuvent vous accompagner au quotidien pour ce genre d'opérations sensibles et délicates. **Contactez-nous pour mettre en œuvre correctement votre « Solution de sauvegarde » au 514-830-8184 (101#).**

"'Unexpected error.' It stopped being 'unexpected' after the first ten times it happened."

CartoonStock.com

Vendredi, le 24 juin 2022
Bonne Saint-Jean !