Cism Gestion Informatique

Le Journal TECHNO

Septembre 2022

Nouveautés et Tendances

Déjà la Rentrée 2022, nous espérons que vous avez passé de belles vacances !

L'équipe de CISM était en Mode Recharge afin d'être en forme pour célébrer, cette année, 25 ans d'existence et d'innovations !

C'est le 2 septembre 2022 que CISM Gestion Informatique soulignait ses 25 ans.

Nous marquerons ce ''quart de siècle de présence'' dans l'industrie informatique avec le « Concours #CISMcelebre25ans ». Aussi, nous vous invitons à surveiller le calendrier de nos évènements à venir.

Septembre 2022

Publication mensuelle de **Bernard Houde,** Président et Expert-Conseil de **CISM Gestion Informatique**

Notre MISSION est d'aider les entreprises à se doter d'un environnement informatique sans problème, avec des solutions nouvelles en matière de Sécurité Avancée, Serveurs, Logiciels, Cloud & Surveillance en temps réel. Nos mots d'ordre sont : **Efficacité**, **Fiabilité** et **Sécurité**.

Les 4 Formations

Que Vous Devez Absolument Faire Avec TOUS Vos Employés

C'est la rentrée ! Nos enfants retournent en classe et ils réapprendront les informations de l'année précédente pour s'assurer qu'ils ont pu conserver ces connaissances. Il n'y a rien de mal à avoir besoin d'un recyclage, et cela est vrai pour les étudiants comme pour vos employés.

Si votre personnel n'a pas suivi de FORMATION sur les « Pratiques de Cybersécurité » de votre entreprise au cours de la dernière année, c'est le moment idéal pour les mettre à jour. Ils ne peuvent pas se défendre contre les cybermenaces s'ils ne savent pas comment s'y prendre. Voilà pourquoi il est si important que votre équipe ait adhéré à une culture de cybersécurité et soit consciente des menaces potentielles qui pourraient avoir un impact sur votre entreprise.

Les cybermenaces sont de toutes formes et de toutes tailles, mais **la majorité des cyberattaques réussies sont attribuées à une erreur humaine**, qui est la principale raison pour laquelle vos employés ont besoin d'une formation sur la cybersécurité au moins 1 fois par an. Un manque de formation peut exposer votre entreprise à des pirates et à d'autres cyberattaques par le biais de courriels de « phishing », de mots de passe faibles, d'une navigation non sécurisée, etc., ce qui met en péril l'ensemble de votre entreprise. De plus, dans de nombreux cas, votre « assurance de Cybersécurité » ne couvrira pas vos réclamations si vos employés n'ont pas suivi de formation. Enfin, vos clients ne veulent assurément pas faire affaire avec une entreprise qui ne protège pas leurs informations. Peu importe la taille de votre entreprise, vous devez faire un effort pour vous assurer que tous vos employés ont suivi une formation en cybersécurité. Cependant, si vous n'avez jamais formé votre équipe à la cybersécurité et que vous ne savez pas quels sujets aborder, ne vous inquiétez pas car nous avons dressé une liste des sujets les plus importants à traiter.

Sécurité du mot de passe

Tous les employés de chaque entreprise ont leur propre identifiant pour accéder aux systèmes, aux données ou à l'Internet de l'entreprise. Lors du choix des mots de passe pour ces connexions, **les employés doivent utiliser des mots de passe forts et uniques** qui utilisent des lettres, chiffres, signes de ponctuation et autres caractères spéciaux (pour un total de 12 caractères minimum). Vous devez aussi vous assurer que vos employés changent régulièrement leurs mots de passe. **Pour une couche de sécurité supplémentaire, nous vous suggérons fortement**

Suite à la page 2

Suite de la page 1

d'utiliser l'authentification multi facteur afin que vous sachiez que ceux qui se connectent à un compte sont ceux qu'ils prétendent être.

Courriel

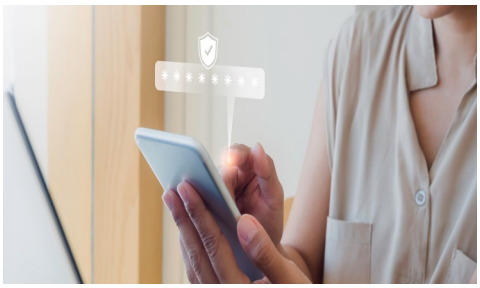
Vos employés doivent se méfier des courriels provenant d'adresses extérieures à l'entreprise. Lorsque vos employés consultent leurs courriels, ils ne doivent pas ouvrir les courriels de personnes qu'ils ne connaissent pas ou avec qui ils n'ont pas communiqué par le passé. À moins qu'ils ne sachent exactement d'où vient le courriel, ils ne doivent pas ouvrir de liens ou de pièces jointes qu'il contient. Et même s'ils connaissent l'expéditeur, ils doivent toujours se méfier car souvent les « hackers » vont emprunter l'identité de fournisseurs connus tels que Purolator, UPS ou Amazone.

Médias sociaux

Les comptes personnels des médias sociaux d'un employé ne doivent jamais être configurés via une adresse électronique d'entreprise. Lorsqu'ils publient sur les réseaux sociaux, vos employés doivent être prudents quant à ce qu'ils publient concernant le travail. Ils ne doivent pas divulguer d'informations privées sur votre entreprise ou vos clients sur les réseaux sociaux. S'ils le faisaient, cela pourrait être dévastateur pour la réputation de votre entreprise ainsi que pour votre cybersécurité.

Protection des données de l'entreprise

En résumé, vos pratiques de cybersécurité sont en place pour protéger les données de votre entreprise, de vos clients et de vos fournisseurs, de plus, vos employés ont l'obligation légale et réglementaire de protéger les informations sensibles. **Une indifférence téméraire pour la protection des informations de l'entreprise peut rapidement entraîner la faillite de votre entreprise ainsi que des poursuites judiciaires.**



Instaurer de solides pratiques de cybersécurité et s'assurer que votre équipe en est consciente grâce à la formation est le meilleur moyen de protéger votre entreprise contre les cybermenaces. En mettant en place une formation sur ces 4 sujets, vous serez sur la bonne voie pour développer une culture cyber-sécurisée. Sachez que **CISM Gestion Informatique** détient l'expertise et les solutions pour vous aider à sensibiliser et former vos employés, pour de l'accompagnement, communiquez simplement avec Bernard au **514-830-8184** (101#).

> " Instaurer de solides pratiques de cybersécurité & s'assurer que votre équipe en est consciente grâce à la formation est le meilleur moyen de protéger votre entreprise contre les cybermenaces. "

LA PRESSE

Publié le 2 juillet 2022
par KARIM BENESSAIEH

Protection des données personnelles
En quoi la nouvelle loi vous touche

Après des années d'attente et une 1ère mouture morte..., Ottawa a finalement présenté à la mi-juin sa loi protégeant les données personnelles.

Amendes pouvant atteindre 25 millions pour les entreprises fautives, droit au contrôle des données pour les simples citoyens et encadrement de l'intelligence artificielle ne sont que les fers de lance de cette loi complexe.

La Presse a demandé à 2 expertes de la vulgariser, pour en savoir davantage, cliquez sur le lien suivant : lapresse.ca/affaires/economie/2022-07-02/protection-des-donnees-personnelles/en-quoi-la-nouvelle-loi-vous-touche.php

Un Audit De Cybersécurité GRATUIT Révélera Où Votre Réseau Informatique Est Exposé & Comment Protéger Votre Entreprise Dès Maintenant

Sans frais ni obligation, notre équipe hautement qualifiée d'experts en informatique se rendra à votre bureau et effectuera un " Audit complet de cybersécurité " (à l'insu de votre fournisseur actuel, si vous le souhaitez) pour découvrir les failles de la sécurité informatique de votre entreprise.

Une fois l'audit terminé, nous préparerons un « **Rapport des résultats personnalisé** » qui révélera des vulnérabilités spécifiques et fournira un « **Plan d'action prioritaire** » pour résoudre rapidement ces problèmes de sécurité. Ce rapport et ce plan d'action devraient être une véritable révélation pour vous, car presque toutes les entreprises, pour lesquelles nous l'avons fait, découvrent qu'elles sont complètement exposées à différentes menaces dans quelques secteurs.

Inscrivez-vous Gratuitement à notre Audit De Cybersécurité via
cisminformatique.com/guides-gratuits/
ou appelez notre bureau au (514) 830-8184 (101#)

Pleins feux sur nos précieux clients

Première entreprise canadienne de livraison « décarbonnée » qui livre de tout, tout le temps, avec une flotte électrique innovante.

Courant Plus rend **plus agile**, **plus vert** et **plus intelligent** le transport des marchandises à Montréal, grâce à leur flotte de véhicules électriques (vélos-cargos, voitures, camionnettes et camions). Enveloppe, colis ou palette, que ce soit une urgence ou une habitude, leur flotte se déploie selon les besoins logistiques de leurs différents clients dans le Grand Montréal.

Dernièrement, **Courant Plus** remerciait CISM d'avoir réagi et répondu rapidement à une de leurs demandes de soutien informatique.

Courant Plus fait confiance à CISM pour ses **Services informatiques gérés**.

Soyez « Cyber Smart »

(#BeCyberSmart)

Nos Meilleurs Conseils de Sécurité du Mois

CONSEIL #4 - Les DANGERS de Dropbox et d'applications de synchronisation de fichiers

Lorsque vos employés travaillent à domicile, ils ont besoin d'**accéder aux fichiers importants** de votre entreprise. Il est facile de regarder des solutions de partage de fichiers dans le Cloud grand public comme Dropbox, OneDrive et Google Drive. Mais, lisez ce qui suit !

Ces applications représentent une énorme menace pour votre entreprise, car les données de l'entreprise peuvent être diffusées à grande échelle sans contrôle central des informations partagées avec quiconque. Plus de 7 MILLIONS de comptes Dropbox ont déjà été piratés, permettant aux cybercriminels d'accéder au réseau d'entreprises.

De plus, si votre entreprise a accès et/ou stocke des données financières ou autres données sensibles. L'utilisation d'applications de partage comme celles-ci est une violation claire des lois sur la violation des données et la conformité. NE LES UTILISEZ PAS POUR LES DONNÉES DE VOTRE ENTREPRISE et **n'utilisez que des applications de partage de fichiers de qualité professionnelle approuvées par votre entreprise**.

CONSEIL #5 - Vos employés laissent-ils cette porte grande ouverte ?

La plupart des employés ont des réseaux sans fil installés chez eux. Contrairement au Wi-Fi de votre entreprise, de nombreux utilisateurs à domicile sont tolérants quant à la création de réseaux sans fil sécurisés, **laissant une porte secrète ouverte aux pirates**. Les signaux Wi-Fi sont souvent diffusés au -delà des maisons de vos employés et dans les rues. Le piratage au volant est populaire parmi les cybercriminels. Des conseils pour sécuriser les points d'accès Wi-Fi :

- Utilisez un cryptage plus fort et un mot de passe plus complexe;
- Masquez le nom de votre réseau sans fil;
- Utilisez un pare-feu.

Ces mesures de sécurité ne sont pas difficiles à mettre en place. Si besoin, me joindre au **514-830-8184** (101#), je serai heureux de vous aider à installer vos employés à distance.

De plus, si vous voulez davantage de conseils pour configurer des réseaux de travail à domicile sécurisés, consultez notre rapport gratuit << cisminformatique.com/11-mesures-de-securite-critiques-teletravail/ >>.

Bernard Houde
Président et Expert-Conseil

*Je suis **Bernard Houde**, passionné de protéger et éduquer les gens en **CyberSécurité**. Depuis 25 ans, nous gérons les Systèmes informatiques de nos clients à distance, des **PME** de la région de **Montréal** comptant de **10 à 100 ordinateurs.** 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)

4. Tenez vos logiciels à jour.
Téléchargez régulièrement les mises à jour suivantes : systèmed'exploitation, navigateur, logiciel de courrier électronique, logiciel antivirus & tous les autres logiciels utilisés sur vos ordinateurs/serveurs.

5. Sauvegardez vos données régulièrement.
Localisez-les dans un lieu éloigné de votre ordinateur, ainsi en cas de vol ou feu, vous aurez toujours accès à vos précieuses données. Idéalement, sauvegardez-les journalièrement sur Internet.

Saviez-vous que ...

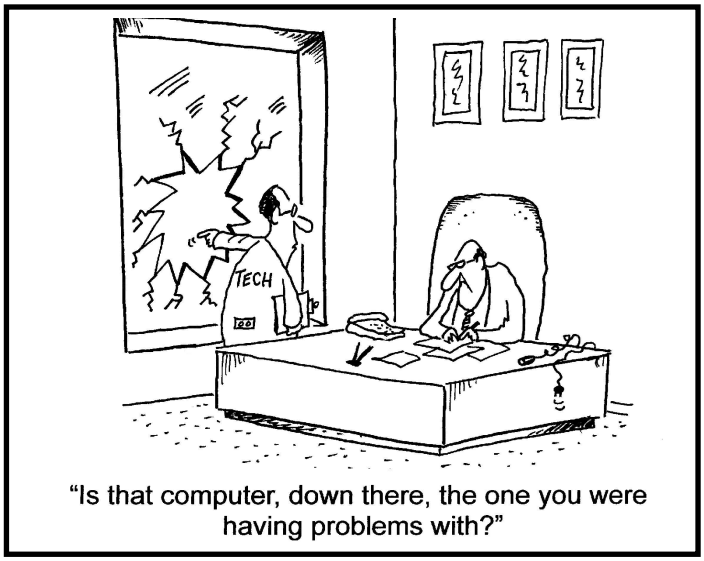
Si vous possédez ou exploitez une PME, vous connaissez probablement certaines des différentes méthodes que les cybercriminels utiliseront pour tenter de voler des informations sensibles à votre entreprise, mais de nouvelles menaces font la une présentement.

Un rapport récent de CyberCatch a vu le fournisseur de plateforme de cybersécurité examiner 20 000 petites entreprises sélectionnées au hasard aux États-Unis pour détecter les vulnérabilités pouvant être exploitées par les cybercriminels.

Il a constaté que le "spoofing", "clickjacking" et "sniffing" sont de nouvelles méthodes exploitées. Que signifient réellement ces termes ?

• **L'usurpation d'identité** se produit lorsqu'un cybercriminel utilise une fausse adresse IP pour se faire passer pour quelqu'un qui a accès au système privé de l'entreprise.
• **Le détournement de clics** survient lorsqu'un utilisateur clique sur quelque chose à l'écran qui semble inoffensif mais qui est en fait malveillant.
• **Le reniflage** a lieu lorsque des pirates interceptent le trafic d'un réseau pour accéder à des données non chiffrées.

Il est important de se tenir au courant de toutes les nouvelles méthodes utilisées par les cybercriminels afin de protéger votre entreprise.



"Is that computer, down there, the one you were having problems with?"

Nouveau guide! ➡ **"7 Signes Que Votre Fournisseur Informatique Ne Vous Convient Plus"**

[Téléchargement Gratuit Maintenant ICI via notre SITE WEB au menu Ressources] afin d'éviter d'être pris au dépourvu lors de l'externalisation de n'importe quel Service Informatique, d'un projet ou du Soutien Technique requis par votre entreprise.