Quelqu'un a piraté votre courriel !

Guide d'urgence

Compte courriel compromis



Dany Chouinard
Nicolas Lamoureux

Première Édition Québec
2025

Introduction - Pourquoi ce guide existe et comment l'utiliser

Bonjour, nous sommes là pour vous aider.

Ce guide a été créé par deux spécialistes qui comprennent exactement ce que vous vivez en ce moment. Je suis Nicolas Lamoureux, Architecte du changement et des transformations, je facilite la gouvernance et simplifie le numérique pour les organisations, et mon collègue Dany Chouinard est Architecte Senior & Responsable expert en Cybersécurité, Leader technologique. Ensemble, nous aidons régulièrement des amis ou de la famille, avec de petites entreprises comme vous, à traverser cette épreuve difficile.

Nous savons que vous vous sentez probablement dépassé, inquiet et peut-être même en colère. C'est tout à fait normal. Se faire pirater son compte courriel, c'est comme si quelqu'un entrait chez vous et fouillait dans vos affaires personnelles. Cette violation de votre espace professionnel crée un stress énorme, surtout quand votre gagne-pain dépend de la confiance de vos clients.

Pourquoi ce guide est-il gratuit ? Parce que nous croyons que tous les entrepreneurs ET tous les citoyens méritent d'avoir accès aux bonnes informations pour protéger leurs informations personnelles et financières, peu importe leur budget. Nous avons vu trop de propriétaires de petites entreprises perdre des clients ou fermer boutique à cause d'un incident de sécurité qui aurait pu être géré correctement, et trop de citoyens perdre leurs économies ou voir leur identité volée.

Ce guide s'adresse autant aux entrepreneurs qu'aux particuliers. Que vous soyez propriétaire d'une petite entreprise préoccupé par vos clients, ou un citoyen dont le courriel personnel a été piraté, les étapes de sécurisation sont essentiellement les mêmes. La différence principale : si vous n'êtes pas entrepreneur, vous pouvez ignorer les sections spécifiques aux clients et à la communication professionnelle, mais toutes les autres étapes (sécurité bancaire, nettoyage des appareils, nouveaux mots de passe, etc.) s'appliquent parfaitement à votre situation personnelle.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Adaptation pour les particuliers : Remplacez mentalement "clients" par "famille et amis", "entreprise" par "finances personnelles", et "réputation professionnelle" par "sécurité personnelle". L'approche et les outils restent identiques.

Comment utiliser ce guide : Chaque section est conçue pour vous accompagner étape par étape, sans vous submerger. Nous utilisons un langage simple, sans jargon technique. Quand vous terminez une étape, cochez-la dans la liste - cela vous donnera un sentiment d'accomplissement et vous permettra de voir vos progrès.

Suivez l'ordre des priorités : certaines actions sont urgentes (aujourd'hui), d'autres peuvent attendre quelques jours.

Rappelez-vous : Vous n'êtes pas seul dans cette situation. Des milliers d'entrepreneurs vivent la même chose chaque année, et la grande majorité s'en sortent plus forts qu'avant. Ce guide vous donnera les outils pour non seulement résoudre la crise actuelle, mais aussi mieux protéger votre entreprise à l'avenir.

Nicolas Lamoureux: https://www.linkedin.com/in/nicolaslamoureuxqc/

Dany Chouinard: https://www.linkedin.com/in/danychouinard/

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Actions IMMÉDIATES (À faire aujourd'hui)

Respirez profondément. Oui, c'est une crise, mais vous allez vous en sortir.

Nous savons que votre première réaction est probablement la panique. C'est humain. Mais voici la bonne nouvelle : en agissant rapidement et méthodiquement aujourd'hui, vous allez transformer cette crise en opportunité de renforcer la sécurité de votre entreprise. Des milliers d'entrepreneurs avant vous ont vécu exactement la même situation et ont non seulement survécu, mais sont devenus plus forts.

Votre nouvelle réalité temporaire : Pendant les prochains jours, vous allez fonctionner différemment. Ce n'est pas permanent, c'est juste le temps de remettre tout en ordre. Pensez à cela comme à une rénovation de votre maison - c'est dérangeant sur le moment, mais le résultat final sera meilleur qu'avant.

Pourquoi commencer par les finances : Votre argent, c'est l'oxygène de votre entreprise. En sécurisant vos finances en premier, vous vous donnez la tranquillité d'esprit nécessaire pour gérer le reste calmement. C'est comme mettre un pansement sur une blessure avant de nettoyer - on arrête d'abord le saignement.

SÉCURITÉ FINANCIÈRE - PRIORITÉ ABSOLUE

Arrêter les paiements Interac

- Connectez-vous à votre compte bancaire en ligne OU allez en succursale
- Annulez tous les virements Interac automatiques programmés
- Changez votre mot de passe bancaire en ligne
- Activez les notifications par SMS pour tous les mouvements sur vos comptes

Important : Ne faites plus AUCUN achat en ligne jusqu'à réception de la nouvelle carte

Annuler votre carte de crédit

Cette action va vous sauver potentiellement des milliers de dollars. Les pirates utilisent souvent les informations volées dans les heures qui suivent. En agissant maintenant, vous leur coupez l'herbe sous le pied.

- **Téléphonez IMMÉDIATEMENT** à votre banque (numéro au dos de votre carte)
- **Dites exactement ceci :** "Ma carte de crédit doit être annulée immédiatement - mon compte courriel a été piraté"
- **Demandez une nouvelle carte** avec un nouveau numéro
- **Demandez aussi** que toutes les transactions des 48 dernières heures soient vérifiées

Ce que vous ressentirez : Un grand soulagement après cet appel. C'est normal - vous venez de reprendre le contrôle de la situation.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Verrouillage de dossier de crédit - La protection ultime

L'arme nucléaire contre l'usurpation d'identité.

Le verrouillage de crédit va encore plus loin que l'alerte de fraude. C'est comme mettre un cadenas inviolable sur votre dossier de crédit - PERSONNE ne peut ouvrir de nouveau compte à votre nom, même avec toutes vos informations personnelles.

Comment ça fonctionne : Votre dossier devient complètement inaccessible pour toute nouvelle demande de crédit. Les banques ne peuvent même pas le consulter sans votre autorisation expresse.

Pour verrouiller votre dossier :

Equifax Canada :

- Appelez : 1-800-465-7166
- Dites : "Je veux verrouiller mon dossier de crédit"
- Coût : Gratuit
- Vous recevrez un code PIN à conserver précieusement

TransUnion Canada :

- Appelez : 1-877-713-3393
- Même processus qu'Equifax
- Également gratuit

IMPORTANT - Ne pas oublier : Vous devrez déverrouiller temporairement votre dossier quand vous aurez besoin de :

- Demander une carte de crédit
- Renouveler votre hypothèque
- Financer un véhicule
- Louer un appartement (vérification de crédit)
- Souscrire à certains services (téléphonie, internet)

Truc pratique : Notez dans votre calendrier les dates importantes (renouvellement d'hypothèque, etc.) pour vous rappeler de déverrouiller temporairement.

Temps de déverrouillage : 15 minutes par téléphone, effectif immédiatement.

Cette protection vous donne : La tranquillité d'esprit absolue - il est maintenant impossible d'ouvrir un compte à votre nom sans votre participation active.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

RAPPORT À LA POLICE



Le plus grand succès des pirates ? Votre silence.

Les cybercriminels comptent sur une chose : que vous gardiez cette attaque secrète par honte ou par peur de nuire à votre réputation. C'est exactement ce qui leur permet de continuer à opérer dans l'ombre et de s'attaquer à d'autres entrepreneurs comme vous. En brisant ce silence, vous devenez un héros pour tous les propriétaires de petites entreprises qui pourraient être leurs prochaines victimes.

Votre responsabilité envers vos clients : Vos clients vous font confiance avec leurs informations personnelles et leurs paiements. En signalant cette fraude officiellement, vous leur montrez que vous prenez cette responsabilité au sérieux. Vous transformez un moment de vulnérabilité en démonstration de leadership et d'intégrité.

Mais surtout, vous jetez une lumière sur des criminels qui agissent dans l'ombre. Chaque rapport de police aide les enquêteurs à identifier des patterns, à remonter des filières et à protéger d'autres victimes. Votre action aujourd'hui pourrait littéralement sauver l'entreprise d'un autre entrepreneur la semaine prochaine. C'est un acte de solidarité entrepreneuriale.

Déposer une plainte officielle

- **Appelez :** Service de police de votre ville OU Sûreté du Québec
- **Numéro d'urgence non-urgent :** 310-4141 (partout au Québec)
- **Centre antifraude du Canada :** 1-888-495-8501
- **Dites :** "Je veux déposer une plainte pour fraude informatique et usurpation d'identité"

Important : Demandez le numéro de votre **rapport de police** - vous en aurez besoin pour les assurances et la banque.

Ce que vous ressentirez après : Un sentiment de fierté et de reprendre le pouvoir. Vous venez de passer de victime à acteur du changement.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

CONTACT URGENT AVEC VOS CLIENTS

Voici le moment où vous transformez une crise en avantage concurrentiel.

La plupart des entrepreneurs qui vivent cette situation cachent le problème par peur de perdre des clients. Grosse erreur. En contactant proactivement vos clients, vous démontrez un niveau de professionnalisme et de transparence que vos concurrents n'ont probablement jamais montré. Vous ne perdrez pas de clients - vous en gagnerez le respect et la loyauté.

Votre responsabilité sociale : En appelant vos clients, vous ne protégez pas seulement votre entreprise, vous protégez des familles québécoises contre la fraude. Ces criminels utilisent souvent votre carnet de contacts pour cibler vos clients. Votre appel pourrait empêcher qu'une grand-mère se fasse soutirer ses économies ou qu'une jeune famille perde l'argent de ses vacances.

Le message que vous envoyez : "Je prends soin de mes clients même quand ça me coûte du temps et des efforts." C'est le genre d'attitude qui fidélise une clientèle à vie et qui génère du bouche-à-oreille positif.

Préparer votre liste de clients

Voyez cela comme une campagne de marketing de crise - mais en mieux, parce que c'est authentique.

- Sortez votre carnet d'adresses/contacts téléphoniques
- Préparez une liste de TOUS vos clients des 2 dernières années
- Incluez leur nom, numéro de téléphone et services fournis

Script d'appel pour vos clients

"Bonjour [nom du client], c'est [votre nom]. J'appelle pour vous informer d'une situation urgente. Mon compte courriel a été piraté par des criminels. Si vous avez reçu des courriels de ma part demandant des paiements ou des informations personnelles dans les derniers jours, NE RÉPONDEZ PAS et supprimez-les immédiatement.

Pour votre sécurité :

- N'envoyez plus de virements Interac à mon ancienne adresse courriel
- Ne donnez aucune information personnelle par courriel
- J'ai déposé un rapport de police (donnez le numéro si vous l'avez)
- Pour nos prochaines communications, appelez-moi directement au [votre numéro de téléphone]
- Je vous recommande d'utiliser un antivirus le plus rapidement possible sur vos ordinateurs pour vous assurer que les pirates ne vous ont pas envoyé de virus à vous aussi."

Résultat garanti : Vos clients vont raccrocher en se disant "Wow, voilà quelqu'un en qui je peux avoir confiance."

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Actions DANS LES 48 HEURES

SÉCURISER VOS APPAREILS

Pourquoi cette étape est cruciale : Les pirates ont peut-être installé des "mouchards" (logiciels espions) sur vos appareils pour voler vos mots de passe futurs. C'est comme s'ils avaient posé des micros dans votre bureau - il faut les détecter et les enlever avant de reprendre vos activités normales.

Changement de mentalité : Vous devenez maintenant quelqu'un qui prend la sécurité au sérieux. Cette habitude vous protégera pour le reste de votre vie d'entrepreneur et impressionnera vos clients professionnels.

Scanner tous vos ordinateurs et appareils

Sur Windows (étapes détaillées) :

1. **Télécharger Malwarebytes (gratuit) :**
    - Ouvrez votre navigateur (Chrome, Firefox, Edge)
    - Tapez exactement : **malwarebytes.com**
    - Cliquez sur "Téléchargement gratuit"
    - **IMPORTANT :** Ne téléchargez jamais depuis Google - allez directement sur le site officiel
    - Cliquez sur le fichier téléchargé (en bas de votre écran ou dans "Téléchargements")
    - Suivez les étapes d'installation (cliquez toujours "Suivant")
2. **Faire le scan :**
    - Une fois installé, ouvrez Malwarebytes
    - Cliquez sur "Scanner maintenant" (gros bouton bleu)
    - **Allez prendre un café** - ça prend 30-60 minutes
    - Si des menaces sont trouvées, cliquez "Supprimer la sélection"
3. **Télécharger un antivirus permanent :**
    - Allez sur **bitdefender.com**
    - Choisissez "Bitdefender Antivirus Free Edition"
    - Installez de la même façon que Malwarebytes
    - Lancez un scan complet

Sur Mac (étapes détaillées) :

1. **Télécharger CleanMyMac :**
    - Allez sur **cleanmymac.com**
    - Cliquez "Télécharger gratuitement"
    - Ouvrez le fichier .dmg téléchargé
    - Glissez l'icône CleanMyMac dans le dossier Applications
    - Ouvrez CleanMyMac depuis Applications
    - Cliquez sur "Malware" puis "Scanner"

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Sur téléphone/tablette :

iPhone/iPad :

- Appuyez sur "Réglages" (icône grise avec engrenages)
- Appuyez sur "Général"
- Appuyez sur "Mise à jour logicielle"
- Si une mise à jour apparaît, appuyez "Télécharger et installer"
- **Branchez votre appareil** - ça peut prendre 1 heure

Android :

- Ouvrez "Google Play Store" (icône colorée)
- Tapez "Bitdefender Mobile Security" dans la barre de recherche
- Appuyez sur "Installer"
- Une fois installé, ouvrez l'app
- Appuyez sur "Scanner maintenant"

Ce que vous pourriez voir : Ne paniquez pas si les logiciels trouvent des choses. C'est normal et c'est exactement pourquoi on fait cette étape. Laissez les programmes nettoyer automatiquement.

Temps total nécessaire : Comptez 2-3 heures pour tout faire, mais vous pouvez vaquer à vos occupations pendant que les scans tournent.



Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

CRÉER UN NOUVEAU COMPTE COURRIEL

Votre renaissance numérique commence ici.

Créer un nouveau courriel, c'est comme déménager dans une nouvelle maison après un cambriolage. Vous repartez à zéro, mais cette fois avec un système de sécurité à la fine pointe. Ce nouveau courriel va devenir le cœur sécurisé de votre entreprise.

Changement de perspective : Vous ne "perdez" pas votre ancien courriel - vous l'abandonnez comme on abandonne une voiture accidentée. Votre nouveau courriel sera bien mieux protégé et donnera une image plus professionnelle.

Créer une nouvelle adresse courriel professionnelle

Choisissez un nom qui inspire confiance :

Options recommandées :

- **Gmail :** nomprenom.entreprise2025@gmail.com
- **Outlook :** votrenom.pro2025@outlook.com

Exemples concrets :

- marie.tremblay.comptable2025@gmail.com
- jean.martin.plombier2025@outlook.com
- sophie.roy.consultante2025@gmail.com

Pourquoi ajouter "2025" ? Ça montre que vous êtes à jour, moderne, et ça évite que votre nom soit déjà pris.

Étapes de création (Gmail - 10 minutes) :

1. **Allez sur gmail.com**
2. **Cliquez "Créer un compte"** puis "Usage personnel"
3. **Remplissez vos informations :**
    - Prénom et nom de famille
    - Nom d'utilisateur : votrenom.entreprise2025
    - Mot de passe : Utilisez votre gestionnaire de mots de passe !
4. **Ajoutez votre numéro de téléphone** (obligatoire pour la sécurité)
5. **Gmail va vous envoyer un code par SMS** - entrez-le
6. **Acceptez les conditions**

Étapes similaires pour Outlook.com

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Configuration de sécurité (CRUCIAL - ne sautez pas cette étape !)

L'authentification à double facteur (2FA) - Votre garde du corps numérique :

Comment ça fonctionne : Même si un pirate devine votre mot de passe, il ne pourra pas entrer sans votre téléphone. C'est comme avoir deux clés différentes pour ouvrir votre coffre-fort.

Activation du 2FA sur Gmail :

1. **Cliquez sur votre photo** (coin supérieur droit)
2. **Cliquez "Gérer votre compte Google"**
3. **Dans le menu de gauche, cliquez "Sécurité"**
4. **Cherchez "Validation en 2 étapes"** et cliquez dessus
5. **Cliquez "Commencer"**
6. **Entrez votre mot de passe**
7. **Ajoutez votre numéro de téléphone**
8. **Google vous envoie un code** - entrez-le
9. **Cliquez "Activer"**

Configuration de récupération :

- **Utilisez votre numéro de téléphone** comme méthode de récupération principale
- **JAMAIS votre ancien courriel compromis** - ce serait comme donner une clé de votre nouvelle maison à votre cambrioleur !
- **Ajoutez un courriel de récupération secondaire** (peut-être celui d'un proche de confiance)

Test final : Déconnectez-vous et reconnectez-vous pour vérifier que tout fonctionne. Vous devriez recevoir un code par SMS.

Ce que vous venez d'accomplir : Vous avez maintenant un compte courriel plus sécurisé que celui de 90% des entreprises. Félicitations !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Changer TOUS vos mots de passe

La réalité brutale : Si les pirates ont accès à votre courriel, ils peuvent probablement deviner ou récupérer vos autres mots de passe. C'est le moment de faire le grand ménage et de repartir sur des bases solides.

Pourquoi TOUS les mots de passe : Imaginez que votre trousseau de clés soit tombé entre les mains d'un cambrioleur. Même s'il n'a utilisé qu'une clé, vous changeriez toutes les serrures, non ? C'est exactement la même logique ici.

Pourquoi un mot de passe différent partout : Si vous utilisez le même mot de passe sur 10 sites et qu'un seul site se fait pirater, les criminels peuvent instantanément accéder à vos 9 autres comptes - c'est comme utiliser la même clé pour votre maison, votre auto, votre bureau et votre coffre-fort.

Changez immédiatement les mots de passe pour :

- Tous vos autres comptes courriels (Gmail, Outlook, etc.)
- Comptes bancaires en ligne
- Réseaux sociaux (Facebook, LinkedIn, etc.)
- Services de stockage (Google Drive, Dropbox, etc.)
- Comptes de facturation/comptabilité
- Tout service lié à votre entreprise

Règles de sécurité absolues à appliquer immédiatement :

Un mot de passe différent partout : Si vous utilisez le même mot de passe sur 10 sites et qu'un seul site se fait pirater, les criminels peuvent instantanément accéder à vos 9 autres comptes - c'est comme utiliser la même clé pour votre maison, votre auto, votre bureau et votre coffre-fort.

Activez l'authentification à double facteur (MFA) partout où c'est offert : Dès que vous voyez "Activer la vérification en 2 étapes" ou "MFA" sur un site, activez-le immédiatement - c'est gratuit et ça rend votre compte 99% plus sécurisé.

Changez TOUTES vos adresses de récupération : Sur chaque compte, allez dans les paramètres de sécurité et remplacez votre ancien courriel compromis par votre nouvelle adresse sécurisée - sinon les pirates peuvent encore récupérer l'accès à vos comptes "par la porte de service".

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

STOP ! Avant de commencer, laissez-moi vous sauver des heures de frustration

Le problème : Créer 15-20 mots de passe différents et complexes, puis s'en souvenir, c'est mission impossible pour un cerveau humain normal.

La solution magique : Un gestionnaire de mots de passe

Imaginez cela comme un coffre-fort numérique ultra-sécurisé :

1. **Vous n'avez qu'une seule clé à retenir** (votre mot de passe maître)
2. **Le coffre-fort crée automatiquement des mots de passe impossibles à deviner** (comme "X9#mK7@pL2$vN4!78dtfa74!*&")
3. **Il remplit automatiquement vos informations** quand vous visitez un site web
4. **Il fonctionne sur tous vos appareils** - ordinateur, téléphone, tablette

Comment ça marche concrètement :

Étape 1 : Vous allez sur **1password.com** ou **bitwarden.com** (gratuit)

Étape 2 : Vous créez UN SEUL mot de passe maître super fort

La technique des "mots de passe québécois"

Forts ET faciles à retenir !

Le secret : Utilisez des paroles de chansons québécoises que vous connaissez par cœur, puis transformez-les avec quelques règles simples. Résultat : des mots de passe ultra-sécurisés que votre cerveau retient naturellement !

Pourquoi c'est génial : Votre gestionnaire de mots de passe va créer des mots de passe automatiquement, mais vous avez quand même besoin d'un mot de passe maître TRÈS fort pour y accéder. Cette technique vous permet de créer ce mot de passe maître parfait.

Exemples concrets avec des classiques québécois :

1. "Une chance qu'on s'a" - Jean-Pierre Ferland

- **Transformation :** Remplacez quelques lettres par des chiffres et ajoutez des symboles
- **Résultat :** `1ChanceQu0nS'a!`
- **Pourquoi c'est fort :** 14 caractères, majuscules, minuscules, chiffres, symboles
- **Pourquoi c'est facile :** Vous chantez cette chanson depuis 20 ans !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

2. "Passe-moé la puck" - Les Colocs

- **Paroles complètes :** "Passe-moé la puck, j'irai marquer un but"
- **Transformation :** Gardez la structure, remplacez quelques lettres
- **Résultat :** `Passe_M0e_la-puck,J'irai_Marquer_1But!`
- **Pourquoi c'est fort :** 35 caractères - même la NSA aurait du mal !
- **Pourquoi c'est facile :** Pure fierté québécoise mémorisée !

3. "J'aurais voulu être un artiste" - Starmania

- **Transformation :** Ajoutez des symboles significatifs pour vous
- **Résultat :** `J'aurai$vouluêtreunartiste%`
- **Pourquoi c'est fort :** Accents + symboles = cauchemar pour les pirates
- **Pourquoi c'est facile :** Luc Plamondon l'a gravé dans votre mémoire !

Vos règles de transformation simples (exemple) :

- Remplacez le "o" par "0" (zéro)
- Remplacez le "i" par "1"
- Ajoutez un "!" à la fin
- Remplacez "et" par "&"
- Utilisez "$" pour les "s" importants

Créez le vôtre maintenant :

1. **Choisissez une chanson québécoise** que vous fredonnez sous la douche
2. **Prenez une phrase** de 4-12 mots
3. **Appliquez 2-3 transformations** simples
4. **Testez-le** - pouvez-vous le retaper 3 fois de suite ?

Résultat magique : Un mot de passe de 25+ caractères impossible à craquer, mais que vous n'oublierez jamais parce qu'il fait partie de votre ADN culturel québécois !

Bonus culturel : Chaque fois que vous tapez votre mot de passe, vous supportez la musique québécoise dans votre tête. C'est de la cybersécurité patriotique !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Un gestionnaire de mots de passe (suite)

Étape 3 : Le gestionnaire génère automatiquement des mots de passe comme "M8#kP9@vL3$nQ7!" distinct pour chaque site

Étape 4 : Quand vous visitez votre banque, il tape automatiquement ce mot de passe compliqué

Résultat : Vous avez des mots de passe de niveau militaire partout, mais vous ne retenez qu'un seul mot de passe simple !

Installation rapide (5 minutes) :

1. Allez sur **bitwarden.com** (gratuit et excellent)
2. Cliquez "Commencer"
3. Créez votre compte avec un mot de passe maître fort
4. Téléchargez l'extension pour votre navigateur
5. Téléchargez l'app sur votre téléphone

Maintenant, changez vos mots de passe un par un :

1. Allez sur le site (ex: votre banque)
2. Cliquez "Mot de passe oublié"
3. Quand on vous demande un nouveau mot de passe, laissez Bitwarden en générer un automatiquement
4. Bitwarden sauvegarde automatiquement le nouveau mot de passe

Temps nécessaire : 2-3 heures pour tout faire, mais c'est un investissement qui vous fera gagner des heures chaque mois pour le reste de votre vie !

Ce que vous ressentirez après : Un sentiment incroyable de contrôle et de sécurité. Plus jamais vous ne direz "Quel était mon mot de passe déjà ?"

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Actions DANS LA SEMAINE

OBLIGATIONS LÉGALES - LOI 25 DU QUÉBEC

Respirez - nous allons naviguer cela ensemble, étape par étape.

Cette section peut sembler intimidante, mais c'est normal. Beaucoup d'entrepreneurs découvrent ces obligations pour la première fois lors d'un incident comme le vôtre. L'important, c'est que vous êtes maintenant au courant et que vous pouvez agir de façon éclairée.

Changement de mentalité : Au lieu de voir cela comme une menace supplémentaire, voyez-le comme une opportunité de vous conformer et de montrer à vos clients que vous prenez leurs données au sérieux. Cela peut devenir un avantage concurrentiel.

Pourquoi cette information est importante pour vous

La réalité : En tant qu'entrepreneur québécois, vous pourriez avoir des obligations légales suite au piratage de votre compte courriel, surtout si des informations personnelles de vos clients ont été compromises. Mieux vaut le savoir maintenant que de l'apprendre plus tard !

La bonne nouvelle : En ayant suivi ce guide jusqu'ici, vous avez déjà pris plusieurs mesures qui vont dans le bon sens de la conformité.

Ce que dit la Loi 25 du Québec (en termes simples)

La Loi 25 établit des règles que les entreprises doivent suivre pour protéger les informations personnelles de leurs clients et réagir correctement en cas de problème.

Vos obligations potentielles pourraient inclure :

- **Évaluer rapidement la situation** et prendre des mesures pour protéger vos clients
- **Déterminer le niveau de risque** pour les personnes concernées
- **Aviser les autorités** (Commission d'accès à l'information) dans certains cas
- **Informer vos clients** si leurs données ont été compromises
- **Documenter l'incident** dans un registre

Important à retenir : Ces obligations dépendent de votre situation spécifique - le type d'informations compromises, le nombre de clients affectés, la nature de votre entreprise.

Pourquoi vous ne devez pas paniquer

Les sanctions peuvent sembler effrayantes (amendes pouvant aller jusqu'à plusieurs millions), mais elles visent les entreprises qui ignorent complètement leurs obligations ou agissent de mauvaise foi. Vous, vous êtes en train de faire les bonnes choses !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Votre prochaine étape (simple et claire)

Nous ne pouvons pas vous donner de conseils juridiques - **nous ne sommes pas avocats**. Mais nous pouvons vous guider vers les bonnes ressources :

Action immédiate recommandée :

1. **Visitez quebec.ca** et recherchez "Loi 25" pour l'information officielle
2. **Consultez cai.gouv.qc.ca** (Commission d'accès à l'information)
3. **Si vous avez des doutes, parlez à un avocat** spécialisé en protection des données

Perspective rassurante : La plupart des petites entreprises qui agissent de bonne foi et prennent les mesures appropriées n'ont pas de problèmes majeurs avec ces obligations. L'important, c'est d'être au courant et d'agir correctement.

Vous n'êtes pas seul : Des milliers d'entrepreneurs québécois naviguent ces mêmes obligations. Les ressources gouvernementales sont là pour vous aider, pas pour vous punir.

Résultat final : En vous informant maintenant, vous transformez une obligation légale potentiellement stressante en démonstration de votre professionnalisme et de votre respect pour vos clients.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

OBLIGATIONS LÉGALES - LOI FÉDÉRALE CANADIENNE

Une deuxième couche de protection - mais pas de stress supplémentaire !

Si vous pensiez que la Loi 25 du Québec était la seule à considérer, il y a aussi une loi fédérale canadienne qui pourrait s'appliquer à votre situation. Mais respirez - vous n'êtes pas en train de vous noyer dans la paperasse légale, vous êtes en train de devenir un expert en conformité !

Changement de perspective : Au lieu de voir cela comme une complication, considérez que le Canada a mis en place plusieurs niveaux de protection pour vous ET vos clients. C'est un système pensé pour vous soutenir, pas pour vous punir.

Pourquoi cette information vous concerne aussi

La réalité simple : Si votre entreprise traite des données personnelles de clients (même juste leurs noms et courriels), la **Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)** pourrait aussi s'appliquer à votre situation.

La bonne nouvelle : Les principes sont très similaires à ceux de la Loi 25 - vous n'apprenez pas un système complètement différent !

Ce que dit la loi fédérale (version simple)

En gros, cette loi dit la même chose que la Loi 25, mais à l'échelle canadienne :

Vos obligations potentielles incluent :

- **Évaluer rapidement si l'incident présente un "risque de préjudice grave"** pour vos clients
- **Aviser le Commissaire à la protection de la vie privée du Canada** dans certains cas
- **Informer les personnes concernées** si leurs données ont été compromises
- **Tenir un registre détaillé** de tous les incidents de sécurité
- **Maintenir des mesures de sécurité appropriées** pour protéger les données

Facteurs d'évaluation du risque :

- La sensibilité des informations (un numéro d'assurance sociale vs. une adresse courriel)
- La probabilité que ces informations soient utilisées malicieusement

Les sanctions (pour vous situer)

Amendes possibles : Jusqu'à 100 000$ pour non-respect des obligations de notification.

Perspective rassurante : Ces sanctions visent les entreprises qui ignorent volontairement leurs obligations, pas celles qui font de bonne foi les efforts appropriés comme vous êtes en train de le faire.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Comment naviguer entre les deux lois

Votre approche simple :

1. **Consultez les deux** - les obligations provinciales ET fédérales
2. **Suivez les exigences les plus strictes** entre les deux
3. **Documentez tout** ce que vous faites (vous êtes déjà sur la bonne voie !)

Votre action pratique (pas de panique !)

Nous ne sommes toujours pas des avocats - nous vous guidons vers les bonnes ressources :

Prochaines étapes simples :

1. **Visitez priv.gc.ca** (site du Commissaire à la protection de la vie privée du Canada)
2. **Cherchez "atteinte à la sécurité"** dans leurs ressources
3. **Si nécessaire, consultez un avocat** qui connaît BOTH les lois provinciale et fédérale

Astuce pratique : Souvent, en respectant les exigences de la Loi 25 (qui sont généralement plus détaillées), vous respectez automatiquement une bonne partie des exigences fédérales.

Ce que vous devez retenir : Vous n'êtes pas en train de jongler avec des systèmes contradictoires - vous suivez des couches de protection qui se complètent. En agissant de bonne foi et en vous informant correctement, vous êtes sur le bon chemin.

Résultat final : Vous devenez un entrepreneur qui comprend et respecte toutes les règles du jeu, ce qui vous donne un avantage énorme sur vos concurrents qui ignorent ces obligations !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

COMMUNICATION OFFICIELLE

Le moment de transformer votre transparence en avantage concurrentiel.

Cette étape va sembler contre-intuitive, mais elle est géniale : au lieu de cacher le problème, vous allez en faire une démonstration publique de votre professionnalisme. Vos concurrents cachent leurs problèmes - vous, vous montrez comment vous les gérez. Cette différence va marquer vos clients pour longtemps.

Changement de mentalité : Vous passez de "j'espère que personne ne le saura" à "je montre à tout le monde comment un vrai professionnel gère une crise". C'est la différence entre un amateur et un entrepreneur mature.

Pourquoi cette communication vous rend plus fort :

- Vos clients voient que vous prenez leurs intérêts à cœur
- Vous devancez les rumeurs et contrôlez le narratif
- Vous démontrez votre intégrité et votre transparence
- Vous éduquez vos contacts sur la cybersécurité (ils vous en seront reconnaissants)

Envoyer un courriel officiel à tous vos contacts

Timing parfait : Envoyez ce courriel quand vous avez terminé toutes les étapes précédentes. Vos clients recevront un message de quelqu'un qui a la situation bien en main, pas de quelqu'un en panique.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Objet : URGENT - Changement d'adresse courriel suite à piratage

Message type :

"Chers clients et partenaires,

Je vous informe que mon compte courriel [ancienne adresse] a été compromis par des cybercriminels. Je communique avec vous immédiatement par souci de transparence et pour protéger vos intérêts.

Actions que j'ai prises : ✓ Rapport déposé à la police du Québec (rapport #[numéro]) ✓ Nouveau compte courriel ultra-sécurisé créé avec authentification à double facteur ✓ Tous mes systèmes ont été nettoyés par des logiciels professionnels ✓ Toutes mes informations bancaires ont été sécurisées

Pour votre protection :

- N'ouvrez plus les courriels provenant de mon ancienne adresse [ancien courriel]
- Utilisez uniquement ma nouvelle adresse : [nouvelle adresse]
- En cas de doute sur l'authenticité d'un courriel, téléphonez-moi au [numéro de téléphone]
- Je recommande fortement d'installer un antivirus sur vos appareils par précaution

Ce que cela change pour vous : Absolument rien dans nos services. Mon engagement envers la qualité et la sécurité reste inchangé - il est même renforcé.

Cette expérience m'a permis de renforcer considérablement la sécurité de mon entreprise. Vos informations et nos communications futures seront mieux protégées qu'elles ne l'ont jamais été.

Je m'excuse pour les inconvénients et vous remercie de votre compréhension et de votre confiance continue.

Cordialement, [Votre nom] [Nouveau courriel] [Numéro de téléphone]

P.S. Si cette situation vous préoccupe pour votre propre entreprise, n'hésitez pas à me demander conseil - je serais heureux de partager ce que j'ai appris."

Le génie de ce message : Vous terminez en position de force, comme un expert qui peut maintenant aider les autres. Vous transformez une faiblesse en expertise !

Réactions attendues : 90% de vos clients vont vous respecter davantage après ce message. Plusieurs vont même vous remercier pour votre transparence et demander des conseils de sécurité.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Mettre à jour vos comptes professionnels

Votre renaissance professionnelle - l'occasion rêvée de rafraîchir votre image.

Ne voyez pas cette étape comme une corvée, mais comme une campagne de rebranding gratuite ! C'est l'excuse parfaite pour moderniser votre présence professionnelle et montrer que votre entreprise évolue constamment. Vos concurrents font ces mises à jour une fois par décennie - vous, vous le faites maintenant parce que vous êtes proactif.

Changement de mentalité : Au lieu de subir cette mise à jour, vous la dirigez. Vous profitez de l'occasion pour améliorer votre image de marque et montrer votre dynamisme.

Plan d'action par priorité :

1. Réseaux sociaux professionnels (Jour 1-2)

- **LinkedIn :**
  - Modifiez votre section "Coordonnées"
  - Ajoutez une note dans votre résumé : "Suite au renforcement de ma cybersécurité, mon nouveau courriel professionnel est [nouvelle adresse]"
  - **Bonus :** Partagez un post sur l'importance de la cybersécurité pour les PME - vous passerez pour un expert !
- **Facebook Entreprise :**
  - Mettez à jour la section "À propos"
  - Changez les informations de contact
  - Publiez une mise à jour rassurante pour vos abonnés

2. Annuaires d'entreprises (Jour 3-4)

- **Pages Jaunes du Québec**
- **Google My Business** (super important pour le référencement local)
- **Répertoire des entreprises du Québec**
- **Chambres de commerce** (si vous êtes membre)

Truc de pro : Pendant que vous y êtes, vérifiez que toutes vos informations sont correctes et à jour. Profitez-en pour ajouter de nouvelles photos ou mettre à jour votre description !

3. Cartes d'affaires - Votre nouveau look (Jour 5)

Pourquoi c'est génial : Vous allez avoir de toutes nouvelles cartes fraîchement imprimées avec votre nouveau courriel sécurisé. Ça donne une image ultra-professionnelle et moderne !

Suggestions d'amélioration :

- Ajoutez un petit symbole de sécurité (🔒) près de votre courriel
- Mettez "Courriel sécurisé" en petit sous votre adresse
- Profitez-en pour moderniser le design si c'était dû !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

4. Factures et documents officiels (Jour 6-7)

Modèles à mettre à jour :

- **En-têtes de factures**
- **Devis et soumissions**
- **Contrats types**
- **Signatures électroniques**
- **Modèles de courriels récurrents**

Astuce psychologique : Ajoutez une petite ligne en bas de vos factures : "Communications sécurisées - Votre confidentialité est notre priorité". Vos clients remarqueront votre attention à la sécurité !

Organisation efficace : Créez un dossier "Nouveaux modèles 2025" et sauvegardez tous vos nouveaux modèles au même endroit. Supprimez les anciens pour éviter les erreurs.

Ce que vos clients vont remarquer : Votre cohérence et votre attention aux détails. Ils verront que vous ne faites pas les choses à moitié et que vous prenez votre entreprise au sérieux.

Temps total estimé : 3-4 heures réparties sur une semaine, mais vous pouvez en faire un peu chaque jour pendant vos pauses.

Résultat final : Une présence professionnelle rafraîchie et cohérente qui inspire confiance et démontre votre évolution constante !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

SURVEILLANCE ET PROTECTION

Vous devenez maintenant un détective de votre propre sécurité financière.

Cette étape transforme votre rapport à l'argent et à la sécurité. Vous passez de "j'espère que tout va bien" à "je surveille activement mes intérêts". C'est la différence entre conduire les yeux fermés et conduire avec tous vos sens en alerte. Cette nouvelle habitude va vous protéger pour la vie.

Changement de mentalité : Vous n'êtes plus une victime potentielle - vous êtes un gardien vigilant de vos finances. Cette surveillance active va même vous faire découvrir des économies et optimiser vos dépenses !

Surveiller vos comptes bancaires

Votre nouvelle routine matinale - aussi importante que votre café !

Pourquoi 2 semaines intensives : Les criminels utilisent souvent les informations volées dans les 14 jours suivant le piratage. Après cette période, le risque diminue drastiquement. C'est votre "période de haute vigilance".

Routine quotidienne (5 minutes chaque matin) :

1. **Ouvrez vos apps bancaires** ou allez sur les sites web
2. **Vérifiez TOUS vos comptes :**
    - Compte chèque
    - Compte épargne
    - Cartes de crédit
    - Marge de crédit
    - Tout autre produit financier
3. **Cherchez spécifiquement :**
    - Transactions que vous ne reconnaissez pas
    - Montants étranges (même petits - les pirates testent souvent avec 1-5$)
    - Virements inhabituels
    - Nouveaux bénéficiaires de virements Interac

Configurer les alertes automatiques :

Chez la plupart des banques :

1. **Connectez-vous à votre compte en ligne**
2. **Cherchez "Alertes" ou "Notifications"** dans le menu
3. **Activez :**
    - Alerte pour TOUTE transaction (même 1$)
    - Alerte pour les virements Interac
    - Alerte pour les paiements pré-autorisés
    - Alerte pour les connexions au compte
4. **Choisissez :** SMS ET courriel (votre nouveau courriel sécurisé)

Si vous voyez quelque chose de suspect :

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

- **NE PANIQUEZ PAS** - c'est exactement pourquoi vous surveillez !
- **Appelez immédiatement** le numéro au dos de votre carte
- **Dites :** "J'ai une transaction suspecte suite à un piratage de courriel"
- **Ayez en main :** Date, montant, et description de la transaction

Surveiller votre crédit

Votre dossier de crédit - la photo complète de votre santé financière.

Pourquoi c'est crucial : Les criminels utilisent parfois vos informations pour ouvrir des comptes à votre nom (cartes de crédit, prêts, cellulaires). Vous pourriez ne pas le savoir pendant des mois !

Obtenir votre rapport gratuitement :

Option 1 - Equifax Canada :

1. **Allez sur equifax.ca**
2. **Cliquez "Rapport de crédit gratuit"**
3. **Remplissez le formulaire** (ils vont vérifier votre identité avec des questions personnelles)
4. **Vous recevrez le rapport par la poste** en 5-10 jours

Option 2 - TransUnion Canada :

1. **Allez sur transunion.ca**
2. **Cliquez "Rapport de crédit gratuit"**
3. **Même processus qu'Equifax**

Ce qu'il faut chercher dans votre rapport :

- **Nouveaux comptes** que vous n'avez pas ouverts
- **Adresses** que vous n'avez jamais habitées
- **Employeurs** qui ne sont pas les vôtres
- **Demandes de crédit** que vous n'avez pas faites

Placer une alerte de fraude (fortement recommandé) :

Comment ça marche : Une note spéciale est ajoutée à votre dossier. Quand quelqu'un demande du crédit en votre nom, la banque DOIT vous appeler pour confirmer que c'est bien vous.

Pour l'activer :

- **Appelez Equifax :** 1-800-465-7166
- **Dites :** "Je veux placer une alerte de fraude sur mon dossier suite à un piratage"
- **Durée :** L'alerte reste active 6 ans (gratuit !)
- **Effet :** Protection automatique sans effort de votre part

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Ce que vous ressentirez : Un énorme soulagement de savoir que vous avez maintenant un système d'alarme sur toute votre vie financière.

Temps d'investissement : 30 minutes pour tout configurer, puis 5 minutes par jour pendant 2 semaines. Après, vous pourrez réduire à 2-3 fois par semaine.

Résultat : Vous dormez sur vos deux oreilles en sachant que rien ne peut vous arriver sans que vous le sachiez immédiatement !



Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

PRÉVENTION FUTURE

MESURES DE SÉCURITÉ PERMANENTES

Félicitations ! Vous êtes maintenant plus blindé que 95% des entrepreneurs.

Cette crise que vous venez de traverser va faire de vous un entrepreneur plus fort, plus sage et plus respecté. Vous avez maintenant une expertise en cybersécurité que vos concurrents n'ont pas. Utilisez-la comme avantage concurrentiel !

Votre nouvelle identité : Vous n'êtes plus quelqu'un qui "espère ne pas avoir de problèmes" - vous êtes quelqu'un qui se prépare activement au succès et à la sécurité.

Sauvegardes régulières - Votre police d'assurance numérique

La règle d'or : Si vous ne pouvez pas vous permettre de perdre cette information, elle doit être sauvegardée en 2 endroits différents.

- **Sauvegardez vos données importantes** sur un disque dur externe (déconnecté d'internet quand pas utilisé)
- **Service cloud recommandé :** iDrive.com (chiffrement militaire, prix abordable)
- **Fréquence :** Une fois par semaine pour les documents importants, quotidien pour les données critiques

Éducation continue - Votre formation permanente d'expert

Vous êtes maintenant un expert en sécurité - continuez à apprendre !

- **Ne jamais cliquer sur des liens suspects** dans les courriels - quand en doute, allez directement sur le site
- **Vérifiez toujours l'adresse de l'expéditeur** - les fraudeurs font des fautes subtiles (gmai1.com au lieu de gmail.com)
- **Méfiez-vous des demandes urgentes** d'argent ou d'informations personnelles - les vrais organismes donnent du temps
- **Mettez à jour régulièrement** vos logiciels et systèmes - programmez-le le premier lundi du mois

Votre nouvelle réputation : Vos clients vont commencer à vous demander des conseils de sécurité. Partagez généreusement votre expertise !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

CONCLUSION



Vous venez d'accomplir quelque chose d'extraordinaire.

En suivant ce guide, vous avez transformé l'une des pires expériences qu'un entrepreneur puisse vivre en démonstration de leadership, de transparence et de professionnalisme. Vous avez protégé vos clients, sécurisé votre entreprise et acquis une expertise précieuse.

Ce que vous avez vraiment accompli :

- Vous avez pris le contrôle d'une situation de crise au lieu de la subir
- Vous avez renforcé la confiance de vos clients par votre transparence
- Vous avez développé des systèmes de sécurité de niveau professionnel
- Vous avez contribué à la lutte contre la cybercriminalité
- Vous êtes devenu une référence en sécurité pour votre entourage

Avertissement important : Nous ne garantissons pas le succès absolu de cette méthode, car chaque situation de piratage est unique. Cependant, ce guide est basé sur les meilleures pratiques reconnues de l'industrie de la cybersécurité et les principes éprouvés de gestion du changement organisationnel.

Sources et références utilisées :

- **Centre canadien pour la cybersécurité :** cyber.gc.ca
- **Centre antifraude du Canada :** antifraudcentre-centreantifraude.ca
- **Malwarebytes Security :** malwarebytes.com
- **Bitdefender Research :** bitdefender.com
- **1Password Security :** 1password.com
- **Bitwarden Security :** bitwarden.com
- **Équifax Canada :** equifax.ca
- **TransUnion Canada :** transunion.ca

Notre engagement : Nous continuerons à mettre à jour ce guide selon l'évolution des menaces et des meilleures pratiques. Votre sécurité et votre succès entrepreneurial nous tiennent à cœur.

Dernière pensée : Dans six mois, quand vous regarderez en arrière, vous réaliserez que ce piratage a été un tournant positif dans votre parcours entrepreneurial. Vous êtes maintenant mieux équipé, plus conscient et plus fort qu'avant.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

CHECKLIST COMPLÈTE -
COCHEZ CHAQUE ÉTAPE ACCOMPLIE

ACTIONS IMMÉDIATES (Jour 1)

□ **Carte de crédit annulée** et nouvelle commandée
□ **Comptes bancaires sécurisés** - virements Interac annulés
□ **Notifications bancaires activées** (SMS + courriel)
□ **Mot de passe bancaire changé**
□ **Rapport de police déposé** - Numéro de rapport : _____
□ **Liste des clients préparée** (2 dernières années)
□ **Appels d'urgence aux clients prioritaires** terminés

ACTIONS DANS LES 48 HEURES (Jour 2-3)

□ **Malwarebytes installé et scan complet** effectué sur ordinateur
□ **Antivirus permanent installé** (Bitdefender ou équivalent)
□ **Scan antivirus complet sur téléphone/tablette**
□ **Gestionnaire de mots de passe installé** (Bitwarden/1Password)
□ **TOUS les mots de passe changés** avec le gestionnaire :
□ Comptes courriels secondaires
□ Réseaux sociaux
□ Services de stockage cloud
□ Comptes de facturation
□ Autres services professionnels
□ **Nouveau compte courriel créé** - Adresse : _____
□ **Authentification à 2 facteurs activée** sur le nouveau courriel
□ **Méthodes de récupération configurées** (téléphone uniquement)

ACTIONS DANS LA SEMAINE (Jour 4-7)

□ **Courriel officiel envoyé** à tous les contacts professionnels
□ **Réseaux sociaux professionnels mis à jour** :
□ LinkedIn
□ Facebook Entreprise
□ Autres plateformes
□ **Annuaires d'entreprises mis à jour** :
□ Google My Business
□ Pages Jaunes
□ Chambres de commerce
□ **Nouvelles cartes d'affaires commandées**
□ **Documents officiels mis à jour** :
□ Modèles de factures
□ Contrats types
□ Signatures électroniques
□ **Surveillance bancaire quotidienne activée** (2 semaines)
□ **Rapport de crédit demandé** :

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

□ Equifax Canada
□ TransUnion Canada
□ **Alerte de fraude placée** sur dossier de crédit
□ **Site gouvernemental consulté** (quebec.ca - Loi 25) pour connaître mes obligations spécifiques
□ **Évaluation professionnelle demandée** (avocat si nécessaire) pour ma situation particulière

MESURES PRÉVENTIVES PERMANENTES

□ **Système de sauvegarde configuré** (disque externe + cloud)
□ **Calendrier de maintenance** programmé (1er lundi du mois)
□ **Numéros d'urgence sauvegardés** dans téléphone
□ **Formation continue** en cybersécurité planifiée

NUMÉROS D'URGENCE SAUVEGARDÉS

□ **Votre banque :** _____
□ **Police locale :** 310-4141 (Québec)
□ **Centre antifraude du Canada :** 1-888-495-8501
□ **Equifax Canada :** 1-800-465-7166
□ **TransUnion Canada :** 1-877-713-3393

FÉLICITATIONS !

Vous avez terminé votre transformation en entrepreneur cyber-sécurisé !

EN CAS D'URGENCE FUTURE : Si vous découvrez des activités suspectes, contactez immédiatement la police au 310-4141 (partout au Québec) et votre institution financière.

RAPPEL FINAL : Gardez ce guide précieusement - il pourrait servir à un collègue entrepreneur dans le besoin. Votre expérience peut maintenant aider d'autres !

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux