

Se protéger des tentatives d'usurpation d'identité

Chez Service alimentaire Gordon, nous nous engageons à protéger nos clients, nos employés et nos partenaires contre la fraude et les escroqueries. Des criminels peuvent tenter d'usurper l'identité de notre entreprise ou d'autres organisations de confiance afin d'accéder à vos informations sensibles ou à vos ressources financières. Cette page fournit des informations pour vous aider à identifier et à signaler les communications suspectes.

Comprendre les risques

Les escrocs utilisent diverses tactiques pour inciter les personnes à fournir des renseignements personnels, à effectuer des paiements ou à autoriser l'accès à leurs systèmes. Ces tentatives peuvent prendre de nombreuses formes, mais elles ont souvent un objectif commun : vous inciter à entreprendre une action qui profite à l'escroc.

Les imposteurs peuvent essayer de créer un sentiment d'urgence ou de peur, vous poussant à agir rapidement sans réfléchir. Ils peuvent aussi tenter de gagner votre confiance en prétendant être un représentant légitime de Service alimentaire Gordon ou d'une autre organisation que vous reconnaissez. Ils peuvent sembler dignes de confiance, professionnels et légitimes.

Identifier les communications suspectes

Les communications semblant provenir de Service alimentaire Gordon, même si elles affichent notre logo ou notre numéro de téléphone, ne sont pas toutes légitimes. Voici ce qu'il faut surveiller :

- **Demandes inattendues :** Méfiez-vous des communications non sollicitées vous demandant des renseignements personnels (mots de passe, données bancaires, numéro de sécurité sociale, etc.), la réalisation d'opérations financières ou l'accès à votre ordinateur ou à des systèmes. Les organisations légitimes, y compris Service alimentaire Gordon, ne demanderont jamais d'informations sensibles par courriel ou par appel téléphonique non sollicité.
- **Sentiment d'urgence :** Les escrocs essaient souvent de vous pousser à agir immédiatement, en invoquant un problème urgent ou une offre à durée limitée. Prenez votre temps et ne vous précipitez pas pour prendre une décision.
- **Moyens de communication inhabituels ou inattendus :** Soyez prudent si vous recevez une demande par un moyen inhabituel ou inattendu. Par exemple, si vous communiquez normalement avec Service alimentaire Gordon par le biais d'un portail ou d'une adresse électronique particulière, méfiez-vous d'une demande provenant d'une source différente.

- **Fautes de grammaire et d'orthographe :** Bien que ce ne soit pas toujours un signe irréfutable, de nombreuses communications frauduleuses contiennent des fautes de grammaire et d'orthographe visibles. Il convient de noter qu'au fur et à mesure que les technologies de l'IA progressent, ce genre de faute sera de moins en moins un signe révélateur, mais il faut tout de même garder un œil là-dessus.
- **Incohérences :** Recherchez les incohérences dans la communication. L'adresse courriel ou le numéro de téléphone correspondent-ils aux coordonnées officielles de Service alimentaire Gordon? Le ton ou le style de la communication est-il différent de ce que vous attendez?
- **Demandes de paiement :** Soyez à l'affût de demandes de paiement sous des formes inhabituelles (p. ex. carte-cadeau ou bitcoins).
- **Trop beau pour être vrai :** Si une offre semble trop belle pour être vraie, il s'agit probablement d'une escroquerie.

Quoi faire si vous soupçonnez une fraude

- **Ne répondez pas :** Ne répondez pas à la communication suspecte et ne cliquez sur aucun lien. Évitez de fournir des informations, en particulier des renseignements personnels ou financiers.
- **N'interagissez pas :** Ne communiquez pas avec le demandeur. Si vous recevez une demande qui vous semble suspecte, contactez la personne ou l'entreprise par des moyens de communication confirmés, tels qu'un numéro de téléphone sur le site Web officiel.
- **Vérifiez la communication :** Si vous n'êtes pas certain de la légitimité d'une communication, contactez Service alimentaire Gordon directement par un canal connu et fiable. *N'utilisez pas les coordonnées fournies dans la communication potentiellement suspecte.* Si vous souhaitez vérifier la légitimité d'une communication que vous avez reçue, remplissez le formulaire ci-dessous.
- **Signalez toute activité suspecte :** Veuillez signaler à Service alimentaire Gordon toute tentative d'usurpation d'identité en remplissant le formulaire ci-dessous. Fournissez une copie du courriel, ainsi que d'autres détails pertinents, notamment la date, l'heure, le moyen de communication (s'il ne s'agit pas d'un courriel) et tout contexte spécifique de la communication. Vous pouvez aussi contacter vos services de police locaux, ainsi que le Centre antifraude du Canada.

Domaines frauduleux utilisés jusqu'à présent

- gordonfoodsservices[.]com
- gfs-vendors[.]com
- gfsvendors-sharefiles[.]com
- gordonsfoodsservices[.]com
- halpems[.]com
- gordonfoodservicesinc[.]com
- gordonsfoodservices[.]com
- gfsvendorportal[.]com
- gfsvendorsportal[.]com
- gfsvendorpayportal[.]com
- gfsvendorspaymentportal[.]com
- gfsvendorspaymentsportal[.]com
- gfsvendorspayportal[.]com
- gfsapvendoranalysis[.]com
- gfsapvendorsanalysis[.]com
- gfsvendorssupport[.]com
- gordonfoodservice[.]zendesk[.]com
- primepaymentportal[.]com
- gordonfoodinc[.]com
- gfsvendorsapanalysis[.]com
- verification-gfspayments[.]com
- gfsvendorapanalysis[.]com
- auth-gfs[.]com
- gfsvendoranalysis[.]com
- gordonsfoodsservice[.]com
- gfs-apvendorsanalysis[.]com
- apvendorsanalysis-gfs[.]com
- Verification-gfspayments[.]com
- Gordonfoodservice[.]zendesk[.]com
- Documentation-gfsapvendoranalysis[.]com
- gfs-paymentsystem[.]com
- gordonfoodservice[.]com

Suite à la page suivante

EXEMPLES DE COURRIEL FRAUDULEUX À DES FINS D'ILLUSTRATION

(Les cybercriminels envoient ces faux messages en anglais, quel que soit le destinataire.)

Gordon Food Service
VENDOR DATA INTEGRITY & PAYMENT SECURITY

Vendor Compliance

Date: 14th July 2026
Dear Vendor Partner,

Immediate Action Required: Payment Profile Temporarily Suspended

Our advanced security-monitoring controls for detecting potential business email compromise have identified indicators that the banking information associated with your company's payment profile may have been changed or may no longer match information previously verified with your organization.

As a precautionary security measure intended to prevent the possible misdirection or loss of your company's funds, the payment profile associated with your vendor account has been temporarily suspended.

Current Payment Status

- All pending and future payments are currently on hold.
- The payment profile will remain suspended until the required verification process has been completed.
- No payments will be processed or released while the suspension remains active.

Required Action by Accounts Receivable

An authorized member of your Accounts Receivable team must complete a **one-time identity verification** to confirm your banking information. Please use the QR code or the link below to access the secure verification portal.



Code malveillant
contenant une
fausse page de
connexion
Microsoft

Verify Your Identity

Scan the QR code with your mobile device, or click the button below

After successful verification, you will be prompted to review and confirm your banking information. If any information appears unfamiliar or incorrect, please contact our Vendor Support team immediately.

If the recipient of this notice is not responsible for managing your company's payment information, please forward this notice immediately to the appropriate Accounts Receivable representative.

Where necessary, the matter may also be escalated internally to your Accounting, Finance, Treasury or Controller department.

Important Security Instructions

- Do not send complete banking information, passwords or authentication codes by email.
- Gordon Food Service personnel will not request your portal password or multifactor-authentication code.
- Carefully report any banking information displayed in the portal that your organization does not recognize.
- Use only your organization's trusted portal access method or an official Gordon Food Service website.

This is a mandatory financial-security requirement and should not be treated as a routine administrative request.

Prompt completion is required to prevent further payment delays and reduce the risk of funds being directed to an unauthorized or incorrect account.

Sincerely,
Vendor Data Integrity & Compliance Team
Gordon Food Service

This message was sent by Gordon Food Service Vendor Compliance.
Please retain this notice for your payment-security records.

De : COMPTES FOURNISSEURS GFS

<vendormangement@documentation-gfsapvendoranalysis>

Date : vend. 19 mars. 2024 16 h 57

À : [REDACTED]

Objet : Dernier avis : le paiement sera versé aujourd'hui sur les comptes se terminant par 8984 – Une intervention immédiate est requise en cas d'erreur



Cher partenaire fournisseur,,

Dernier avis : débloquage du paiement prévu aujourd'hui

Le présent message fait suite à notre précédente communication concernant la mise à jour bancaire transmise à votre compte.

*N'ayant **reçu aucune réponse ni objection**, nous procédons conformément aux délais de traitement habituels.*

⚠ Mise à jour concernant le traitement du paiement

Le paiement est en cours de traitement aujourd'hui (19 mars 2026) vers le compte bancaire se terminant par 8984.

Si ce compte n'est **PAS autorisé par votre organisation**, vous devez **nous contacter immédiatement** avant le virement afin d'éviter toute erreur de versement.

Une fois le paiement effectué, le recouvrement peut être retardé et soumis aux procédures bancaires.

Action immédiate requise (en cas d'erreur)

- *Contactez-nous immédiatement*
- *Confirmez les coordonnées bancaires correctes*
- *Fournissez un contact autorisé pour vérification*

URGENT : Contactez le service de conformité des fournisseurs

Équipe chargée de l'intégrité et de la conformité des données fournisseurs

Si vous pensez avoir été victime d'une escroquerie

Si vous pensez avoir fourni des informations à un escroc ou avoir été victime d'une escroquerie, prenez les mesures suivantes :

- **Contactez l'équipe de sécurité de votre entreprise :** Contactez immédiatement l'équipe de sécurité de votre entreprise afin qu'elle puisse enquêter sur l'incident et prendre d'autres mesures si nécessaire.
- **Communiquez avec votre institution financière :** Si vous avez fourni des renseignements financiers, contactez immédiatement votre banque ou votre entreprise de cartes de crédit pour signaler l'incident et prendre des mesures pour protéger vos comptes.
- **Changez vos mots de passe :** Si vous avez fourni des mots de passe ou d'autres identifiants de connexion, changez-les immédiatement pour tous les comptes concernés. Si vous utilisez le même mot de passe, ou un mot de passe similaire, pour d'autres comptes non liés, modifiez-les aussi. Utilisez un gestionnaire de mots de passe et des mots de passe forts et uniques pour chaque compte. Assurez-vous que l'authentification multifacteur est activée pour tous les comptes sensibles.
- **Surveillez vos comptes :** Vérifiez régulièrement vos comptes bancaires, vos relevés de cartes de crédit et autres comptes pour détecter toute activité non autorisée.
- **Envisagez un gel de crédit :** Vous pouvez mettre en place un gel de crédit sur votre dossier de crédit afin d'empêcher les escrocs d'ouvrir de nouveaux comptes à votre nom. Pour ce faire, vous pouvez contacter l'un des trois principaux bureaux de crédit (Equifax, Experian et TransUnion).
- **Portez plainte auprès des autorités :** Signalez l'incident aux autorités compétentes, telles que le Centre antifraude du Canada (antifraudcentre-centreantifraude.ca) ou vos services de police locaux.

Rester informé

Service alimentaire Gordon s'engage à tenir sa communauté informée des dernières tactiques d'escroquerie. Nous mettrons régulièrement cette page à jour avec de nouvelles informations et ressources. Vous pouvez également en savoir plus sur les escroqueries les plus courantes et sur les moyens de vous protéger grâce aux ressources disponibles sur le site du Centre antifraude du Canada ou d'autres agences gouvernementales.

Veillez nous faire part de toute escroquerie ou communication suspecte en remplissant le formulaire [ici](#).