

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
- gfsvendorpayportal[.]com
- gfsapvendoranalysis[.]com
- gfsapvendorsanalysis[.]com
- gfsvendorssupport[.]com
- support@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
- gordonfoodservicellc[.]zendesk[.]com

EXEMPLES DE COURRIEL FRAUDULEUX À DES FINS D'ILLUSTRATION

De : COMPTES FOURNISSEURS GFS

Date : vend. 27 sept. 2024 16 h 57

À : [REDACTED]

Objet : Urgent : Vérification des informations de paiement requise

Bonjour,

Nous avons récemment envoyé un courriel à tous les fournisseurs pour leur demander de vérifier leurs informations bancaires afin de nous assurer que nous disposons de données à jour avant de traiter les paiements. Cependant, nous n'avons pas reçu de réponse de votre part.

Nous avons envoyé un fichier sécurisé contenant vos informations bancaires actuelles pour vérification, mais nous n'avons pas reçu de réponse. Pourriez-vous

nous confirmer que vous avez reçu le fichier contenant vos informations de paiement? Si ce n'est pas le cas, faites-le-nous savoir et nous le renverrons immédiatement.

Cette demande est importante et doit être traitée sans tarder. Tant que nous n'aurons pas reçu le formulaire rempli et les informations mises à jour, nous ne pourrons pas traiter les paiements. Cette mesure est mise en place pour protéger nos processus de paiement.

Veuillez accuser réception dès que possible.

Nous vous remercions de l'attention que vous accordez à la situation.

*Larry Sanders
Gestionnaire, Comptes fournisseurs
account.payable@gordonfoodsservices.com - AP*

*De : COMPTES FOURNISSEURS GFS
Date : lundi 20 janv. 2025 7 h 21
À : [REDACTED]
Objet : Impossible de traiter le paiement*

Bonjour,

Ceci est un nouveau rappel que nous essayons de traiter votre paiement, mais qu'il semble que la vérification de vos informations bancaires n'a pas été effectuée. Par conséquent, les paiements sont actuellement bloqués dans le système et ne peuvent être traités.

Afin d'éviter tout retard supplémentaire, nous vous demandons de bien vouloir terminer immédiatement le processus de vérification en téléversant vos informations bancaires sur le portail de paiement. Cette étape est essentielle pour garantir une transaction rapide et sans heurts.

Nous vous remercions de l'attention que vous portez à cette situation et nous sommes heureux de vous aider si vous rencontrez des problèmes au cours du processus. Veuillez nous avvertir dès que la vérification est terminée.

Merci de votre coopération.

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](#).