Les arnaques et votre petite entreprise:

un guide pour les entreprises

French

Lorsque des arnaqueurs s'en prennent à votre entreprise ou à votre organisation à but non lucratif, cela peut nuire à votre réputation et à vos résultats. Quelle est la meilleure façon de vous protéger ? Découvrez les signaux d'arnaque ciblant les entreprises. Formez ensuite vos employés et vos collègues sur la façon d'éviter les arnaques.

- **Techniques des arnaqueurs**
- **Protégez votre entreprise**
- **Arnaques courantes visant les petites entreprises**
- **Autres pratiques douteuses**

▶ Techniques des arnaqueurs

- **Les arnaqueurs se font passer pour des personnes de confiance.** Ils se font passer pour une entreprise ou un organisme gouvernemental que vous connaissez, afin de vous inciter à leur verser de l'argent. Mais il s'agit d'une arnaque.
- **Les arnaqueurs créent un sentiment d'urgence, vous intimident et vous font peur.** Ils veulent que vous agissiez avant d'avoir eu la possibilité de vérifier leurs affirmations. Ne laissez personne vous presser de payer des sommes ou de donner des informations commerciales sensibles.
- **Les arnaqueurs vous exigent un moyen de paiement spécifique.** Ils exigent souvent un paiement par virement bancaire, par cryptomonnaie ou par carte cadeau. N'effectuez aucun paiement à destination d'une personne exigeant un tel moyen de paiement. C'est une arnaque.

▶ Protégez votre entreprise

Formez votre personnel

- Votre meilleure défense est d'avoir un personnel formé. Apprenez à vos employés à ne pas divulguer de mots de passe ou des informations sensibles par e-mail, même si l'e-mail semble provenir de leur hiérarchie. Expliquez à vos employés comment fonctionnent les arnaques et encouragez-les à consulter leurs collègues en cas de soupçon d'arnaque. Commandez des exemplaires gratuits de cette brochure sur **ftc.gov/bulkorder** et partagez-les avec votre personnel.

Vérifier les factures et les paiements

- Assurez-vous que les procédures de validation des achats et des factures sont claires et faites examiner

attentivement toutes les factures par votre personnel. Faites attention à la manière dont on vous demande de payer et exigez à votre personnel le même niveau d'attention. Si un tiers vous exige un paiement par virement bancaire, cryptomonnaie ou carte-cadeau, abstenez-vous. C'est une arnaque.

Repérez les arnaques liées aux nouvelles technologies

- Les arnaqueurs falsifient souvent leurs numéros de téléphone, ne vous fiez donc pas à l' identifiant de l'appelant. Si vous recevez un SMS ou un courriel auquel vous ne vous attendiez pas, ne cliquez sur aucun lien, n'ouvrez aucune pièce jointe et ne téléchargez aucun fichier. C'est ainsi que les arnaqueurs introduisent des logiciels malveillants dans votre réseau ou essaient de vous convaincre d'envoyer de l'argent ou de partager des informations sensibles. Parfois, les arnaqueurs piratent même les comptes de médias sociaux de personnes que vous connaissez et envoient des messages en apparence légitimes, mais qui sont frauduleux. Pour en savoir plus sur la protection de votre petite entreprise ou de votre organisation à but non lucratif contre les cyberarnaqueurs et les pirates informatiques, consultez le site **Cybersécurité pour les petites entreprises** à l'adresse **ftc.gov/cybersecurity**.

Maitrisez votre collaborateur

- Avant toute collaboration avec une nouvelle entreprise, faites une recherche sur Internet sur son nom en y associant les termes « arnaque » ou « plainte ». Lisez ce que les autres disent de cette entreprise. Demandez conseil à des personnes de confiance. Vous pouvez également bénéficier de conseils gratuit sur le développement commercial via les programmes tels que **SCORE.org**.

▶ Arnaques courantes visant les petites entreprises

Fausses factures et articles non commandés

Les arnaqueurs créent de fausses factures qui donnent l'impression que vous avez commandé des produits ou des services pour votre entreprise. Ils espèrent que la personne responsable du règlement de factures supposera que les factures sont légitimes et effectuera le paiement. Sauf qu'il s'agit de fausses factures. Un arnaqueur peut aussi vous appeler en prétendant vouloir « confirmer » une commande en cours, « vérifier » une adresse ou vous offrir un catalogue ou un échantillon « gratuit ». Si vous répondez par l'affirmative à l'une de ces questions, des articles non commandés arriveront à votre porte, accompagnés d'une demande très pressante de paiement. Abstenez-vous de payer. Et n'oubliez pas que si vous recevez des marchandises que vous n'avez pas commandées, la loi vous autorise les garder et les utiliser gratuitement.

Arnaques à l'inscription et à la publicité en ligne

Les arnaqueurs essaient de vous faire payer une publicité inexistante ou une inscription dans un faux annuaire professionnel. Ils peuvent vous demander vos coordonnées pour une inscription « gratuite », ou vous dire qu'ils veulent simplement « confirmer » vos informations. Plus tard, vous recevrez une grosse facture et l'arnaqueur peut brandir des détails ou même un enregistrement de l'appel précédent pour vous obliger à payer.

Arnaques aux entreprises et aux administrations

Les arnaqueurs se font passer pour des personnes que vous connaissez ou en qui vous avez confiance, et essaient de vous effrayer ou de vous inciter à payer ou à

leur donner des informations. Par exemple:

- Les arnaqueurs disent qu'ils appellent de la part d'une société de services publics et que votre service de gaz, d'électricité ou d'eau est sur le point d'être interrompu à cause d'une (fausse) facture en retard.
- Les arnaqueurs prétendent être des agents du gouvernement et menacent de suspendre votre licence d'exploitation, de vous infliger une amende ou même de vous poursuivre en justice. Ils peuvent prétendre que vous avez des impôts impayés ou que vous devez renouveler une licence ou un enregistrement.
- Certains arnaqueurs vous persuadent d'acheter des affiches de conformité sur le lieu de travail que vous pouvez obtenir gratuitement auprès du Département américain du Travail.
- Certains arnaqueurs vous incitent à payer afin de bénéficier soi-disant de subventions aux entreprises dans le cadre de programmes gouvernementaux, qui sont en fait faux.
- Les arnaqueurs se font passer pour l'Office américain des brevets et des marques et vous menacent de suspension de votre marque si vous ne payez pas immédiatement une taxe. D'autres fois, ils mentent et disent que vous devez de l'argent pour des services d'enregistrement supplémentaires.
- Certains arnaqueurs prétendent appeler de la part d'une société de technologie et menacent de suspendre l'URL de votre site web de votre entreprise si vous ne payez pas immédiatement.

Les arnaques au support technique

Les arnaques au support technique commencent par un appel ou un message alarmant qui s'affiche sur votre écran. Les arnaqueurs se font passer pour des représentants d'une société informatique bien connue et

vous disent votre ordinateur a un problème de sécurité. Leur objectif est de vous soutirer vos sous, d'accéder à votre ordinateur, ou les deux. Ils peuvent vous demander de payer pour régler un problème que vous n'avez pas vraiment, enregistrer votre entreprise à un programme de maintenance informatique inexistant ou inutile, ou se faufiler dans votre réseau pour soutier données confidentielles qu'ils utiliseront pour usurper votre d'identité.

Ingénierie sociale, ameçonnage et logiciel de demande de rançon

Les cyber-arnaqueurs peuvent inciter les employés à leur envoyer de l'argent ou à leur communiquer des informations confidentielles ou sensibles telles que des mots de passe ou des données bancaires. Cela commence souvent par un courriel d'hameçonnage commence par un courriel d'hameçonnage, un contact sur les médias sociaux ou un appel qui semble provenir d'une source fiable par exemple, un superviseur ou un autre employé de haut rang, et qui crée un sentiment d'urgence ou de peur. D'autres courriels peuvent prendre l'apparence des demandes de mise à jour de mot de passe ou à d'autres messages automatisés, mais il s'agit en fait de tentatives de vol d'informations. Les arnaqueurs peuvent également utiliser des logiciels malveillants pour verrouiller les fichiers des organisations et demander une rançon.

Arnaque au coaching d'affaires

Certains arnaqueurs vendent de faux programmes de coaching d'entreprise, en recourant souvent à de faux témoignages, des vidéos, des présentations de séminaires et des appels de télémarketing. Ils promettent de faux résultats stupéfiants si vous payez pour leur système exclusif « éprouvé » pour réussir dans les affaires. Ils peuvent également vous attirer en vous proposant des coûts initiaux peu élevés, pour ensuite

vous demander des milliers de dollars. En réalité, les arnaqueurs abandonnent les entrepreneurs en herbe sans leur accorder l'aide qu'ils recherchaient, et avec des milliers de dollars de dettes.

Modifier les évaluations en ligne

Certains arnaqueurs prétendent pouvoir remplacer les avis négatifs sur votre produit ou service, ajouter des avis positifs ou augmenter votre score sur les sites d'évaluation. Or, la publication de faux avis est illégale. Les directives de la FTC stipulent que les mentions, y compris les évaluations, doivent refléter les opinions et expériences honnêtes de l'auteur de la mention.

Arnaques liées au traitement des cartes de crédit et à la location d'équipement

Certains arnaqueurs promettent des tarifs attractifs pour le traitement des transactions par carte de crédit ou de meilleures offres de location d'équipement. Ces arnaqueurs ont recours à des petits caractères, des demi-vérités et des mensonges purs et simples pour obtenir la signature d'un propriétaire d'entreprise sur un contrat. Certains agents commerciaux peu scrupuleux demandent aux propriétaires d'entreprise de signer des documents vierges. (Refusez) D'autres modifient les conditions une fois le paiement effectué. Demandez à l'agent de vous remettre immédiatement une copie de tous les documents. S'il refuse ou vous fait patienter en vous promettant de vous les envoyer plus tard, c'est peut-être le signe que vous avez affaire à un arnaqueur.

Arnaques aux faux chèques

Certains arnaqueurs vous donnent une raison apparemment plausible de vous payer un chèque en trop. Ils vous demandent ensuite de leur renvoyer la somme supplémentaire, ou de le renvoyer à quelqu'un d'autre. Mais il s'agit d'un faux chèque, même s'il apparaît comme « approuvé » sur votre compte. Le

temps que la banque découvre que le chèque était faux, l'arnaqueur a déjà perçu l'argent que vous lui avez envoyé. Vous serez obligé de rembourser la banque.

▶ Autres pratiques douteuses

Les arnaqueurs se cachent parfois derrière d'autres pratiques douteuses, comme le fait de prétendre offrir des emplois très lucratifs dans le cadre de l'économie parallèle, mais de ne pas tenir leurs promesses d'argent. Ils peuvent aussi essayer de vous vendre des services inutiles en prétendant que vous devez payer pour améliorer le rapport de solvabilité de votre entreprise. Et après une catastrophe naturelle, des entrepreneurs non agréés et des arnaqueurs peuvent se présenter en vous promettant de remettre votre entreprise en état de marche grâce à des réparations rapides, un nettoyage ou un enlèvement des débris qui n'ont jamais eu lieu.

▶ En savoir plus

- Pour plus de conseils sur la protection de votre entreprise contre les arnaques, reportez-vous sur le site **ftc.gov/SmallBusiness**.
- Restez en contact avec la FTC en vous abonnant au Business Blog de la FTC à l'adresse **ftc.gov/subscribe**.

▶ Signalez

- Si vous avez été victime d'une escroquerie, appelez le 877-382-4357, et appuyez sur la touche 3 pour changer de langue, et sur 4 pour choisir le français — ou rendez-vous sur le site **ReportFraud.ftc.gov**
- Alertez le procureur général de votre État. Vous trouverez les coordonnées des personnes à contacter sur **NAAG.org**.

▶ S'engager

- Remarque: votre meilleure défense est d'avoir un personnel formé. Expliquez à votre personnel comment fonctionnent les arnaques.
- Partagez cette brochure avec votre personnel.
- Téléchargez une copie gratuite de cette brochure sur **ftc.gov/languages**.

À propos de la FTC

La FTC a pour ambition d'aider les propriétaires de petites entreprises à éviter les escroqueries, à protéger leurs ordinateurs et leurs réseaux afin de sécuriser les données de leurs clients. Pour obtenir les informations relatives aux petites entreprises, accédez à **ftc.gov/SmallBusiness**. Vous y trouverez des informations sur les escroqueries ciblant les petites entreprises et comment les éviter, ainsi que des informations sur la cybersécurité pour les petites entreprises afin d'aider les propriétaires à maintenir leurs réseaux en sécurité.

Pour obtenir les dernières informations destinées aux petites entreprises, abonnez-vous au blog commercial de la FTC à l'adresse **ftc.gov/subscribe**.

This brochure is part of the FTC's efforts to help small business owners avoid scams. It explains common scams that target small businesses and non-profit organizations, describes scammers' tactics, and provides steps business owners can take to protect their company from scams. Order print copies for free at **ftc.gov/bulkorder**.

FEDERAL TRADE COMMISSION

business.ftc.gov

Juillet 2023