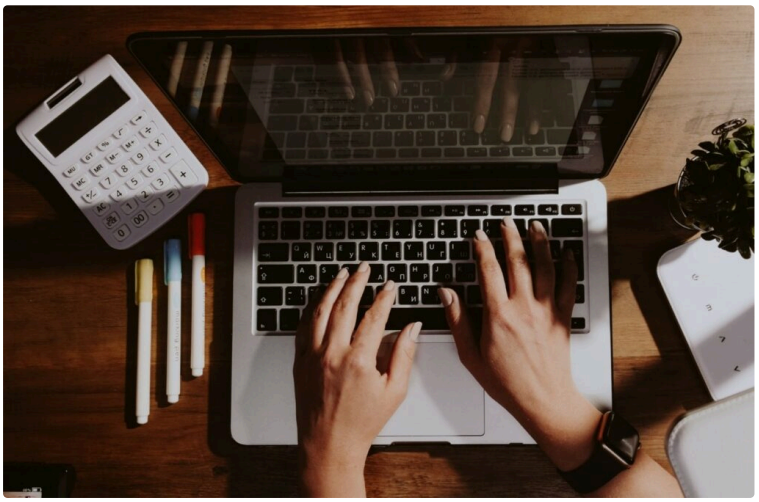
Le journal du Gers

Date de parution: Le mercredi 12 mars 2025 à 20h57

Adresse url de base: https://lejournaldugers.fr/article/82668-securite-se-premunir-contre-lescroquerie-aux-faux-ordres-de-virement-ou-arnaque-au-president

Sécurité : se prémunir contre l’escroquerie aux faux ordres de virement ou « arnaque au président »



Sécurité : se prémunir contre l’escroquerie aux faux ordres de virement ou « arnaque au président »

La préfecture communique :

Ces derniers jours, plusieurs chefs d'entreprises ont signalé aux services de la Préfecture avoir fait l'objet d'une tentative d’escroquerie aux faux ordres de virement.

Le Préfet du Gers souhaite donc rappeler aux acteurs économiques gersois la nécessité d'être extrêmement vigilants devant l'impact potentiellement grave d'une telle fraude.

L’escroquerie aux faux ordres de virement, aussi appelée « l’arnaque au président », connaît régulièrement des variantes. Elle fait de nombreuses victimes parmi les entreprises. Les services de l’État, les collectivités locales et les établissements publics de santé sont également concernés. Quels sont les signaux qui doivent alerter ? Et comment s’en prémunir ? Des gestes simples permettent de décourager les escrocs.

L’arnaque au président consiste pour le fraudeur à contacter une entreprise cible, en se faisant passer pour le président de la société mère ou du groupe. Le contact se fait par courriel ou par téléphone. Après quelques échanges destinés à instaurer la confiance, le fraudeur demande que soit réalisé un virement (en général international), systématiquement non planifié, au caractère urgent et confidentiel. L'employé sollicité s'exécute, après avoir reçu les références du compte à créditer, contrôlé par les fraudeurs.

La dernière variante de cette fraude se déroule en deux étapes :

Le fraudeur usurpe l’identité d’une administration, la direction générale des finances publiques, en utilisant nom, sceaux et timbres de l’Etat (Marianne) et citant des articles législatifs pour prétexter un contrôle auprès d’une entreprise cible. Sous couvert de cette fausse identité, le fraudeur réclame des informations sur l’entreprise et sur ses clients.

Par la suite, le fraudeur se fait passer pour l’entreprise cible auprès de ses clients et annonce un changement de compte bancaire, le paiement des futures factures seront donc payées sur le nouveau compte appartenant au fraudeur.

Plusieurs mesures peuvent être prises pour éviter ce type d’arnaques comme ne pas agir dans la précipitation malgré l’insistance de l’interlocuteur, informer les membres de son entreprise sur l’existence de ces pratiques, lire l’ensemble du document, vérifier via des sources fiables l’identité de l’interlocuteur (Internet, CCI/CMA, infogreffe).

Si ces escroqueries ont lieu tout au long de l’année, elles sont plus fréquentes dans les périodes de trouble ou les périodes de congés profitant ainsi de l’absence des responsables « comptes clients », « comptabilité », « sécurité informatique » plus au fait de ces pratiques.

Voici un aperçu des points d’attention juridique et des moyens pour protéger votre entreprise contre cette menace :

Responsabilité de l’entreprise : en cas de fraude, la responsabilité de l’entreprise peut être engagée si elle n’a pas mis en place des mesures de sécurité adéquates. Il est crucial de documenter toutes les procédures de contrôle interne et de formation des employés pour démontrer que des mesures préventives ont été prises.

Assurance contre la fraude : vérifiez si votre entreprise dispose d’une assurance contre la fraude. Certaines polices d’assurance couvrent les pertes financières dues à des « arnaques au président », mais il est important de comprendre les conditions d'intervention et les exclusions de garantie.

Signalement et poursuites : en cas de fraude, il est essentiel de signaler l’incident aux autorités compétentes, telles que la police et les organismes de régulation financière. La coopération avec les autorités peut non seulement aider à récupérer les fonds, mais aussi à prévenir d’autres fraudes.

Protection des données : assurez-vous que les données sensibles de votre entreprise sont protégées conformément aux réglementations en vigueur, telles que le RGPD (Règlement Général sur la Protection des Données). La protection des données personnelles et financières est un aspect crucial pour éviter les fraudes.

Formation des employés : sensibilisez vos employés aux risques de l'arnaque au président. Organisez des sessions de formation régulières pour leur apprendre à reconnaître les signes de fraude et à réagir de manière appropriée.

Vérification des demandes de virement : mettez en place des procédures strictes pour vérifier les demandes de virement, surtout celles qui semblent urgentes ou inhabituelles. Exigez une confirmation (verbale ou autre) avant d'exécuter toute transaction importante.

Double authentification : utilisez des systèmes de double authentification pour les transactions financières.

Contrôles internes : renforcez vos contrôles internes en séparant les responsabilités. Par exemple, la personne qui initie un virement ne devrait pas être la même que celle qui l'approuve. Cela réduit le risque de fraude interne.

Surveillance des comptes : surveillez régulièrement les comptes bancaires de l'entreprise pour détecter toute activité suspecte. Utilisez des outils de surveillance automatisés pour recevoir des alertes en temps réel en cas de transactions inhabituelles.

Communication sécurisée : encouragez l'utilisation de canaux de communication sécurisés pour les échanges sensibles. Évitez de discuter de transactions financières par e-mail ou téléphone sans vérification préalable.

www.economie.gouv.fr/dgccrf/les-fiches-pratiques/professionnels-agents-publics-attention-larnaque-au-president