Groupement Départemental de la Gendarmerie Nationale

Escroquerie aux fournisseurs par changement de RIB

Le Groupement départemental de la Gendarmerie Nationale nous informe d'une recrudescence de tentative d'escroquerie aux fournisseurs par changement de RIB :

Les fraudeurs procèdent de 2 manières :

La première :

Dans un premier temps, le fraudeur identifie un de vos grands fournisseurs. Il le contacte, en se faisant passer pour votre comptable, votre commissaire aux comptes, etc. et lui demande des informations sur les factures en attente de paiement. Dans un deuxième temps, il vous contacte, en se faisant passer pour votre fournisseur. Il vous notifie alors un changement de compte bancaire, et vous communique les vraies factures, sur lesquelles il aura pris soin de modifier le numéro de compte et les coordonnées téléphoniques. Cette fraude est redoutable, car :

- Elle s'attaque à des **processus normaux** pour l'entreprise (contrairement à la fraude au président) – quoi de plus naturel en effet qu'un paiement fournisseur ?
- La fraude est généralement **détectée trop tard** pour espérer un rappel de fonds, et elle peut durer plusieurs mois, le fraudeur s'arrangeant pour faire patienter le vrai fournisseur.
- Certaines personnes ignorent que généralement, les banques destinataires ne vérifient pas le **nom du bénéficiaire** indiqué dans le virement.

La seconde :

Le procédé est un peu identique, sauf que dans ce cas le fraudeur pirate votre messagerie afin d'obtenir vos factures fournisseurs, avant de vous les retourner en ayant modifié le RIB et en vous le signifiant.

Les montants en jeu dépendent de vos paiements fournisseurs, mais peuvent atteindre des montants très importants (jusqu'à une partie significative de votre chiffre d'affaires !).

Nous vous appelons à la plus grande vigilance et vous rappelons les bons réflexes à adopter, notamment **quelques règles simples à respecter :**

- Réaliser une vérification en cas de changement d'interlocuteur habituel ou en cas de changement de ses coordonnées ;
- Limiter l'accès à la gestion des coordonnées servant aux contre-appels à des personnes habilitées ;
- Apprendre aux collaborateurs à vérifier les adresses mail de leurs correspondants, en étant attentif aux noms de domaines pouvant différer de celui appartenant au fournisseur d'un caractère difficile à détecter. Pour ceci, il peut être utile également d'afficher les en-têtes détaillées du mail.

lien pour apprendre à afficher les en-têtes détaillées de mails pour différentes messageries : https://support.google.com/mail/answer/29436?hl=fr&visit_id=637419822949282623-1748494354&rd=1

- **Authentifier tout changement de compte bénéficiaire** (qui peut vous être notifié par courrier, par lettre recommandée, par mail, sur la facture, par téléphone, etc.) :
  - Demander à la comptabilité fournisseur (ou au service achats) de réaliser un **contre-appel à l'interlocuteur habituel** auprès du fournisseur afin de vérifier la validité du changement de compte ;
  - Bien entendu, ce contre-appel est réalisé en utilisant des **coordonnées sûres**, et non celles communiquées sur la facture ou la notification de modification de compte.

Escroquerie par courrier postal

Le Groupement départemental de la Gendarmerie Nationale nous signale qu'un document envoyé par courrier postal est reçu par plusieurs entreprises sur le territoire national depuis le 24 novembre 2020. Une

société du département a avisé avoir reçu ce courrier. Ce document est une facture au nom de la société "Office Pro" (***annexe 1***).

Bien que cette société existe, le courrier envoyé est une escroquerie. Les références du compte bancaire sont domiciliées sur l'Ile de Malte.

Un appel à la vigilance mérite d'être relayé auprès de vos adhérents tout en leur rappelant les bons réflexes à adopter :

- rester vigilant à la réception d'un courrier ;
- communiquer en interne pour toutes les escroqueries détectées.