



Groupement de Gendarmerie Départementale des Vosges

Attention aux arnaques contre les entreprises



Ce type d'arnaque est fréquente, et elle touche toutes les entreprises, même les plus grandes. Cette arnaque implique que le fraudeur contacte une entreprise cible en se faisant passer pour le président de la société mère ou un haut responsable. Le contact s'établit par mail ou téléphone, et après quelques échanges de confiance, le fraudeur demande un virement international non planifié urgent et confidentiel.

D'autres exemples similaires existent :

- Le fraudeur se fait passer pour l'entreprise cible auprès de ses clients, et annonce un changement de compte bancaire.
- Le fraudeur se fait passer pour une administration de l'État, ou un ministre et demande des paiements urgents et confidentiels.

Récemment une entreprise s'est faite escroquer plus de 200 000 euros grâce à ce type d'arnaque. Un fraudeur se présentant comme un avocat agissant pour une opération confidentielle de reprise d'entreprise, lui a demandé un virement vers l'étranger pour ladite opération. Le gérant s'aperçoit de l'escroquerie suite à des impayés et évite de justesse un second virement de 100 000 euros.

Ces arnaques sont minutieusement préparées par une organisation criminelle qui s'informe longuement sur l'entreprise avant de passer à l'action. Elles ont souvent lieu pendant une période de trouble ou de congés, profitant de l'absence des responsables. Elles piratent les boîtes mails de l'entreprise et connaît parfaitement leur mode de fonctionnement.

Comment se prémunir contre cette arnaque ?



- Informer les membres de l'entreprise de ces types d'arnaques ;
- Ne pas agir dans la précipitation malgré l'insistance de la demande ;
- Toujours lire l'ensemble des documents présentés ;
- Vérifier l'identité de l'auteur de la demande via des sources fiables (internet, CCI, infogreffe ...) ;
- Instaurer des procédures de vérifications et signatures ou d'accords multiples pour les paiements internationaux ;
- Maintenir à jour le système de sécurité informatique.

En cas d'escroquerie

- Identifier les virements ou paiements impliqués dans l'escroquerie ;
- Demander la suspension du paiement ;
- Si des coordonnées bancaires frauduleuses ont été utilisées, demander le blocage ;
- Déposer plainte auprès de la brigade de gendarmerie locale ou le commissariat local, en apportant le maximum d'information (identité de l'auteur, moyen de communication, adresse mail, numéro de téléphone, document transmis ...)