

ALERTE FOVI

Le réseau des référents Cybermenaces de la Police nationale constate une recrudescence des arnaques aux faux ordres de virements. Restez vigilant !



#RCMCYBERTIPS

- Résister aux tentatives d'intimidation et à la pression psychologique.
- En cas de doute, prendre attache directement avec la personne au sein de la société soit physiquement soit avec les coordonnées connues de l'entreprise.
- Se méfier de tout changement de coordonnées téléphoniques ou mails. La communication d'un nouveau numéro à l'indicatif français n'est pas une garantie, tout comme une adresse mail hébergée par un opérateur généraliste.
- Dans ce dernier cas, l'affichage complet de l'entête du mail permettra d'identifier le réel émetteur.
- Désigner un nombre restreint de personnes autorisées à valider les modifications de coordonnées bancaires et téléphoniques.



ALERTE FOVI

#RCMCYBERTIPS

Si le virement a été effectué

- Effectuer en urgence un compte rendu de l'événement à la hiérarchie.
- Contacter immédiatement votre chargé d'affaires afin qu'un retour des fonds soit effectué dans les plus brefs délais.
- Déposer plainte en apportant un maximum d'éléments (entête de mails et leurs contenus, numéros de téléphone utilisés par les escrocs, dates et heures des appels, les éléments confidentiels communiqués aux escroc, etc...), au commissariat le plus proche ou en brigade de gendarmerie.

La Police judiciaire vous propose un point de contact unique pour le territoire
Bretagne et Pays de la Loire

cybermenaces-rennes@interieur.gouv.fr



Le réseau des référents cybermenaces de la Police nationale est une structure innovante composée de :

- Réservistes issus du monde de l'entreprise engagés dans la lutte contre la cybercriminalité
- Policiers spécialisés
- Investigateurs en cybercriminalité
- Professionnels et Institutions partenaires

