

Escroquerie par usurpation d'identité

la détecter, s'en protéger



Les indices

- ◆ Le nom de la société ou des dirigeants est exact mais l'adresse mail utilisée est très légèrement modifiée ou renvoie à une adresse personnelle (par exemple : gmail ou yahoo).
- ◆ La communication avec l'acheteur se fait uniquement par portable ou mail.
- ◆ Après commande, une livraison rapide est exigée, avec paiement à 30 jours.
- ◆ L'adresse de livraison est différente de l'entreprise ayant passé commande.
- ◆ La vente est « à destination » mais le nouveau client impose son choix du transporteur.

Une fois la livraison effectuée, les fraudeurs disparaissent avec la marchandise, sans jamais la régler.

Que faire ?

À LA PRISE DE COMMANDE

- ◆ S'il s'agit d'un client habituel, vérifier l'identité de l'appelant.
- ◆ S'assurer que le mail est authentique en comparant l'extension de l'e-mail avec celle du site officiel ou des contacts mentionnés sur le site.
- ◆ Exiger une commande écrite du client final.
- ◆ Effectuer un contre-appel à la société à partir d'un numéro de téléphone pris dans l'annuaire ou déjà utilisé pour une commande précédente.
- ◆ Proscrire pour la première livraison un départ usine.
- ◆ Vérifier que l'adresse de livraison est identique à l'adresse de facturation.

LIVRAISON

- ◆ Exiger de choisir le transporteur et couvrir ce risque spécifique par une assurance.
- ◆ Si ce n'est pas possible, se renseigner sur le transporteur.
- ◆ Indiquer au transporteur que vous êtes le seul à pouvoir effectuer des modifications sur le lieu de livraison (convenir d'un mot de passe).
- ◆ Le CMR doit être émargé correctement par chaque intervenant.
- ◆ Demander à ce qu'une copie du CMR soit envoyée rapidement par le transporteur.

PAIEMENT

- ◆ Même si le paiement s'effectue par SWIFT, ne pas expédier de marchandise tant que le paiement de la première livraison n'a pas été crédité sur votre compte (un ordre de paiement n'a pas de valeur effective).