

TAPA EMEA Driver Security Guide

TAPA EMEA Copyright © Do Not Copy



FRENCH

TABLE DES MATIÈRES

<u>INTRODUCTION ET ENVIRONNEMENT DE SECURITE DE LA CHAINE D'APPROVISIONNEMENT</u>	<u>3</u>
<u>COMMUNICATION AVEC LA POLICE ET LA DIRECTION</u>	<u>4</u>
<u>TYPES D'ACTIVITÉS CRIMINELLES.....</u>	<u>5</u>
INTRUSION, CAMBRIOLAGE & VOL.....	6
DÉCEPTION.....	8
DÉTOURNEMENT	11
L'ENTRÉE D'IMMIGRANTS ILLÉGAUX	13
CRIMINALITE DES VEHICULES DE LA DERNIERE MILE	15
CYBERCRIMINALITE ET FUITE DE SECURITE DES INFORMATIONS....	17
<u>FONCTIONNALITES ET SOUTIEN DES CENTRES DE DISPATCHING OU DE SURVEILLANCE ET DE REPONSE AUX CONDUCTEURS</u>	<u>19</u>
<u>EUROPEAN EMERGENCY CONTACT NUMBERS.....</u>	<u>21</u>
<u>REFERENCES.....</u>	<u>23</u>
<u>CLAUDE DE NON-RESPONSABILITE POUR LE GUIDE DE SECURITE DU CONDUCTEUR.....</u>	<u>23</u>

Introduction et environnement de sécurité de la chaîne

Le vol de cargaison est un problème majeur à l'échelle mondiale. La plupart du transport de marchandises en Europe se fait par la route. Il en va de même pour les autres pays d'Europe, du Moyen-Orient et d'Afrique. En particulier pour l'Union européenne, le vol de cargaison routière peut être considéré comme une menace pour l'un des principes fondamentaux de l'UE, la libre circulation des marchandises. Les pertes annuelles dues aux vols de cargaison en Europe sont estimées à 8,2 milliards d'euros, soit une valeur moyenne de 6,72 euros par trajet.

- En 2023 seulement, le nombre de vols de cargaison signalés à TAPA EMEA dépasse les 50 000 ; cela représente plus de 140 vols par jour.
- Au cours des trois dernières années, la perte moyenne pour les crimes majeurs signalés avec une valeur de plus de 100 000 euros dépasse un million d'euros.
- Pendant la même période, la valeur des marchandises volées dans les chaînes d'approvisionnement en EMEA toutes les 24 heures est légèrement supérieure à 800 000 euros.
- En Afrique du Sud, il y a eu une légère baisse des détournements de camions enregistrés, mais une augmentation des vols en transit de fonds.
- Parmi ces crimes de cargaison :
 - En moyenne, 80 % sont des vols de camions/remorques.
 - Parmi ces 80 %, 10 % ont lieu dans des parkings non sécurisés.

Tant les attaques opportunistes que les attaques organisées sont susceptibles de se produire pendant le transport routier de cargaison. En ce qui concerne les menaces opportunistes, l'absence « d'offres d'opportunité » est la clé pour réduire ces incidents. D'autre part, comprendre le mode opératoire des réseaux criminels est crucial pour lutter efficacement contre les crimes liés au transport de cargaison. Ces réseaux criminels opèrent au-delà des frontières, utilisant souvent des structures commerciales légales pour leurs activités. Les secteurs comme la construction, l'hôtellerie et la logistique sont particulièrement vulnérables à l'infiltration par le crime organisé.



Communication avec la police et la direction

Une communication efficace avec les autorités policières et la direction des transporteurs est cruciale pour les conducteurs, surtout en cas de situations anormales. Dans ces situations malheureuses, les conducteurs doivent transmettre des informations importantes de manière claire et précise. Les barrières linguistiques peuvent constituer un défi, car les conducteurs peuvent ne pas parler la langue locale. Dans de tels cas, des mécanismes fournis par des centres de surveillance professionnels peuvent aider en utilisant des locuteurs natifs pour communiquer avec les autorités locales. Certains de ces centres de surveillance disposent d'un réseau de centres et de sociétés de sécurité le long des itinéraires des conducteurs pour fournir un soutien en cas d'incidents, soit en offrant des services de sécurité sur place si nécessaire, soit en facilitant l'interaction locale avec la police et les services médicaux d'urgence.

En cas d'incident de sécurité, les conducteurs doivent être capables de communiquer avec précision au moins les informations suivantes à la police :

- Nom du conducteur et numéro d'immatriculation du véhicule
- (camion et remorque)
- Caractéristiques particulières du véhicule (couleur, marque, logos spéciaux, etc.) qui permettront aux forces de police de localiser les véhicules

- Localisation du véhicule (aussi précisément que possible) en utilisant soit le marquage kilométrique de la route, soit la ville/village le plus proche traversé, soit tout point de repère (c'est-à-dire station-service, etc.)
- Type d'incident et si un soutien médical est nécessaire.

La communication avec la direction des transporteurs en cas d'incident doit fournir la même précision et un ensemble minimal d'informations, en se concentrant principalement sur les deux derniers points mentionnés ci-dessus, étant donné que les données des conducteurs et des véhicules sont bien connues des transporteurs.



Types d'activités criminelles

Dans ce Guide de Sécurité des Conducteurs, nous explorerons les types courants d'activités criminelles et fournirons des conseils sur la prévention, la réponse et le signalement.. Selon le dernier rapport d'Europol, il existe 821 réseaux criminels dans l'UE comptant plus de 25 000 membres. Ces réseaux se livrent à divers crimes, notamment le trafic de drogue, la fraude, les crimes contre les biens, le trafic de migrants et la traite des êtres humains. Le trafic de drogue est une activité importante, avec 50 % des réseaux criminels les plus menaçants impliqués, et 36 % se concentrant uniquement sur le trafic de drogue. Nous analyserons également plusieurs types spécifiques d'activités criminelles de manière à présenter uniquement les sujets qui peuvent être directement affectés par les conducteurs et à fournir des orientations avec des actions faciles à comprendre et à retenir que les conducteurs doivent prendre ou éviter lors de tels incidents. Pour la plupart des types de crimes analysés, nous avons également inclus quelques exemples connexes.

MOST TARGETED PRODUCTS – TOP 5 COUNTRIES



South Africa

1. Phones
2. Cash
3. Misc. Electronics
4. Metal
5. Food & Drink



United Kingdom

1. Fuel
2. Food & Drink
3. Tobacco
4. Clothing & Footwear
5. No Load (Theft of truck and/or trailer)



Germany

1. Fuel
2. Metal
3. Tools/Building Materials
4. Auto Parts
5. No Load (Theft of truck and/or trailer)



France

1. Fuel
2. Metal
3. Jewellery/Precious Metals
4. Misc. Electronics
5. Food & Drink



Sweden

1. Fuel
2. Metal
3. No Load (Theft of truck and/or trailer)
4. Cash
5. Food & Drink

Note: TAPA EMEA is recording losses in over 20 TIS product categories. However, across EMEA, most recorded cargo crimes stated the products targeted as unspecified or miscellaneous.

Intrusion, Cambriolage & Vol

Quelle est la menace d'intrusion, de vol à main armée et de vol (de cargaison/carburant)?

Il existe plusieurs situations où les criminels parviennent à pénétrer dans le compartiment de chargement (intrusion) et à voler partiellement la cargaison. Il y a également des cas où les criminels parviennent à voler le camion entier ou la remorque avec la cargaison complète.

Comment prévenir la menace d'intrusion, de vol à main armée et de vol ?

Pour réduire le risque d'intrusion, de vol à main armée ou de vol, il est conseillé de suivre l'itinéraire prévu et d'éviter les arrêts ou les changements non planifiés, car ces événements non planifiés offrent aux criminels l'opportunité recherchée pour attaquer. Bien que suivre le plan ne garantisse pas une sécurité totale, cela diminue considérablement la probabilité de devenir une victime.

De plus, il est recommandé de ne pas arriver trop tôt à l'installation de destination, car attendre à l'extérieur expose à la fois le conducteur et la cargaison aux criminels qui sont actifs dans les parcs logistiques.

De plus, il y a eu une augmentation remarquable des incidents signalés de vol de carburant récemment, impliquant à la fois de petites et de grandes quantités de diesel.

Si vous avez déjà été affecté ou êtes devenu victime d'un incident/cambriolage, veuillez partager le type, l'ampleur, l'emplacement et le type de produits impliqués avec nous via l'adresse e-mail suivante :

tisteam@tapaemea.org.

De cette manière, nous pouvons enregistrer l'incident dans notre base de données TAPA EMEA et aider les autres conducteurs et répartiteurs à répondre aux tendances pertinentes.

THEFT FROM VEHICLE INCIDENT ON 12.03.2024

Incident Details	Place	Product
DATE 12.03.2024	City -	CATEGORY Miscellaneous Electronics
INCIDENT CATEGORY Theft from Vehicle	REGION/ COUNTRY -/ Germany	PRODUCT DETAILS Electrical appliances
MODUS OPERANDI Intrusion	LOCATION TYPE Unclassified Parking	VALUE IN EUR 150,000.00
	LATITUDE/ LONGITUDE 51.401352397921/ 11.719513675255	

Source: TIS database

THEFT FROM TRAILER INCIDENT IN 20.02.2024

Incident Details	Place	Product
DATE 20.02.2024	City Naples	CATEGORY Miscellaneous
INCIDENT CATEGORY Theft from Vehicle	REGION/ COUNTRY -/ Italy	PRODUCT DETAILS Perfumery and Tobacco products
MODUS OPERANDI Intrusion	LOCATION TYPE Unclassified Parking	VALUE IN EUR 2,400,000.00
	LATITUDE/ LONGITUDE 40.8517746/15.2681244	

Source: TIS database

Aires de stationnement sécurisées

Lorsque vous faites des pauses pendant votre trajet, il est recommandé d'utiliser des aires de stationnement sécurisées. Consultez vos répartiteurs avant de commencer votre voyage pour localiser ces aires de stationnement sécurisées le long de votre itinéraire. Les avantages d'utiliser des aires de stationnement sécurisées comprennent :

- Une sécurité renforcée pour le conducteur et la cargaison, réduisant ainsi le risque d'activité criminelle.
- L'accès à des installations de repos et d'hygiène pour aider les conducteurs à se détendre pendant leurs pauses.
- En cas d'incident, les systèmes de sécurité comme les caméras de surveillance peuvent fournir des preuves pour soutenir les enquêtes policières et internes.

Arrêts non planifiés et changements imprévus de trajet

Les criminels cherchent souvent à exploiter toutes les irrégularités de votre itinéraire, les considérant comme des opportunités pour vous attaquer et voler la cargaison. Il est crucial de rester vigilant et de minimiser tout écart ou perturbation non planifié qui pourrait créer de telles opportunités.

Comment réagir en cas d'intrusion, de vol et de menace de vol ?

À faire :

- Protégez-vous. Si vous êtes dans votre cabine, restez à l'intérieur.
- Appelez immédiatement la police.
- Si votre camion est équipé d'un bouton de panique, appuyez dessus, ou essayez de communiquer avec votre centre de surveillance/répartition.
- Rassemblez autant d'informations que possible sur les criminels à partager avec la police.
- Préservez la scène de crime, pour soutenir les équipes d'enquête.
- Si vous devez vous garer à l'extérieur d'une zone de stationnement sécurisée :
 - Positionnez les portes de chargement de votre camion/remorque contre un mur, un bâtiment ou une autre remorque/voiture.
 - Gardez l'arrêt/pause aussi rapide/court que possible.
- Utilisez des bouchons de réservoir verrouillables et des dispositifs anti-siphonnage pour prévenir les vols de carburant.

Ne pas faire :

- NE TENTEZ PAS de défendre la cargaison en confrontant les criminels, car cela peut mettre votre vie en danger.
- NE CHANGEZ PAS votre itinéraire prévu et les arrêts programmés, sauf si nécessaire, et informez votre centre de répartition tout en prenant des mesures de sécurité supplémentaires.
- NE CHANGEZ PAS votre adresse de livraison sans confirmation positive de votre répartiteur.
- NE VOUS EN REMETTEZ PAS aux passants pour vous guider si vous êtes perdu ; il vaut mieux leur demander des informations sur votre emplacement à la place.

Comment signaler la menace d'intrusion, de vol à main armée et de vol ?

Si vous êtes confronté à un incident de sécurité impliquant une intrusion entraînant un vol ou un vol de votre cargaison, signalez-le comme suit ou communiquez les informations suivantes à la police / au centre de surveillance et/ou au centre de répartition :

-  Heure/date/lieu de l'incident
-  Toute blessure ou besoin de soutien médical d'urgence
-  Nom du conducteur / plaques d'immatriculation du camion/remorque
-  Nombre de criminels impliqués
-  Mode opératoire des criminels (comment cela s'est-il produit)
-  Perte estimée de la cargaison

Déception

Quelle est la menace de la tromperie ?

Dans de nombreux cas, les attaquants essaient d'accéder à la cargaison non pas en l'attaquant directement, mais par des moyens détournés. Ce mode opératoire implique l'utilisation de moyens trompeurs pour duper les courtiers, les transporteurs, les expéditeurs et bien sûr les conducteurs afin de remettre une charge aux voleurs au lieu d'une entreprise légitime. Les voleurs se feront passer pour des expéditeurs légitimes, des courtiers, des policiers ou d'autres autorités, voire même des conducteurs, pour obtenir la cargaison. Dans certains cas, les attaquants peuvent cibler les systèmes de sécurité embarqués à bord des véhicules, en essayant de confondre ou de désinformer le conducteur sur l'emplacement de la cargaison. Ils peuvent également intercepter ou bloquer la communication entre le conducteur, le centre de répartition/surveillance ou les autorités policières. L'interception des capteurs et dispositifs à bord des véhicules est une autre tactique utilisée par les attaquants contre les opérations de transport de cargaison.

Les enlèvements de faux chauffeurs représentent environ 2% du total des vols de cargaison en Europe, mais dans certains cas, les pertes sont d'une valeur significative. En novembre 2023, un faux chauffeur se faisant passer pour le véritable chauffeur a réussi à voler des téléphones portables à l'aéroport de Schiphol à Amsterdam, d'une valeur de plus de 1,5 million d'euros.

THEFT OF TRAILER INCIDENT ON 10.11.2023

Incident Details	Place	Product
DATE 10.11.2023	City Reims	CATEGORY Food & Drink
INCIDENT CATEGORY Theft of Trailer	REGION/COUNTRY -/France	PRODUCT DETAILS champagne
MODUS OPERANDI Deception Others	LOCATION TYPE En Route	VALUE IN EUR 600,000.00
	LATITUDE/ LONGITUDE 49.258329/ 4.031696	

Source: TIS database

Comment prévenir la menace de la tromperie ?

- Prévenir l'usurpation d'identité
Pour prévenir l'usurpation d'identité et les actions frauduleuses potentielles des criminels, il est important de rester vigilant et de suivre ces lignes directrices :
 - Si vous êtes arrêté par quelqu'un prétendant être la police ou une autre autorité pour un contrôle, soyez vigilant et envisagez la possibilité d'usurpation d'identité.
 - Si, juste avant d'arriver à l'installation de livraison, un employé de l'entrepôt vous informe que vous devez livrer à un endroit différent, vérifiez toujours les informations avec votre centre de répartition avant de continuer.
- **Éviter le brouillage et le spoofing :**
Le brouillage consiste à bloquer intentionnellement les signaux de communication, rendant les appareils incapables de transmettre ou de recevoir toute forme de communication (appels vocaux, SMS, signaux d'alarme, etc.). Le spoofing, quant à lui, implique que les fraudeurs utilisent des techniques trompeuses pour gagner la confiance des victimes en modifiant les identifiants d'appelants ou en envoyant des messages qui semblent provenir d'une source différente, fiable aux yeux des conducteurs.

On 16 May 2023, cargo thieves attacked and hijacked a truck travelling en route from Port Elizabeth to Cape Town, South Africa. The truck driver was shot and seriously injured.

After taking control of the vehicle, the offenders used a GPS jammer to delay security monitoring services and drove the vehicle to a remote location to offload and steal its cargo.

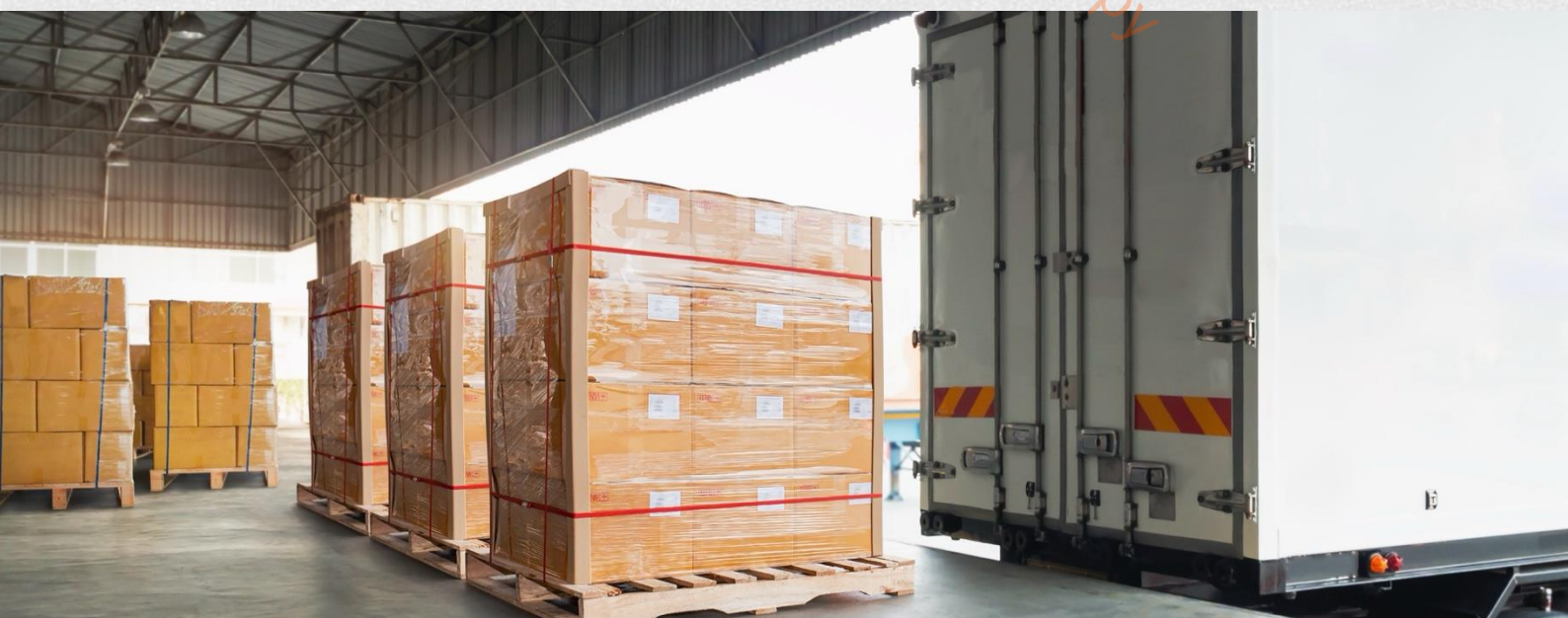
The target: catalytic converters.

This is just the latest in a series of high value and violent attacks on automotive supply chains in the Europe, Middle East & Africa (EMEA) region, with catalytic converters the prime target. In the last 18 months, thefts of catalytic converters have been reported to the TAPA EMEA Intelligence System (TIS) in France, Germany, and the United Kingdom as well as in South Africa. While most crime reports stating this product type do not share financial loss data, these are known to be significant, high value incidents.

Yet, as with so many other types of cargo crime, the number of recorded thefts is believed to represent only a small minority of the total number of incidents taking place.

Le spoofing est souvent utilisé pour tromper les victimes afin qu'elles révèlent des données sensibles ou pour mener des négociations de rançon tout en dissimulant l'identité de l'attaquant. Les réseaux criminels peuvent même proposer des services de spoofing à d'autres criminels.

Dans le transport de marchandises, les criminels utilisent couramment le spoofing GPS pour manipuler l'emplacement affiché sur l'appareil d'un conducteur, les éloignant de leur itinéraire prévu et les rendant vulnérables aux attaques.



- **Vol de véhicules en mouvement (interne et externe)**

Il y a dix ans, Europol a mis en garde contre un nouveau phénomène où des criminels utilisent une méthode de « cheval de Troie » pour accéder aux camions de livraison en se dissimulant dans de grandes caisses en bois. Les caisses marquées comme « Fragile » sont récupérées par les services de livraison de colis. Une fois la caisse à l'intérieur d'un camion, en route vers sa destination finale, les criminels s'échappent de la caisse pour voler des objets de valeur également présents dans le camion, tels que des bijoux, des téléphones ou des appareils électroniques. Des complices suivant à distance simulent ensuite un accident pour arrêter le véhicule, permettant à ceux qui sont cachés à l'intérieur de s'échapper par des trous découpés dans le toit du véhicule.

Les vols de cargaison impliquant des accidents simulés sont assez courants et les vols de camions en mouvement ont également été signalés régulièrement. Cependant, le modus operandi du cheval de Troie décrit ci-dessus était à l'époque un phénomène nouveau.

Un autre modus operandi intéressant est celui où les criminels suivent le camion en mouvement à la même vitesse. Ils se positionnent dans l'angle mort du camion, généralement à l'arrière, où le conducteur ne peut pas les voir dans les rétroviseurs. Ils montent ensuite sur la remorque, coupent les scellés de la cargaison et montent à bord du véhicule pour effectuer le vol. Des complices suivent à une très petite distance fixe derrière le camion attaqué pour recevoir les marchandises volées. À la fin de l'attaque, les attaquants à bord retournent dans leur véhicule et ralentissent pour s'éloigner du camion.

Comment réagir à une menace de tromperie ?

À faire :

- Si vous avez des doutes sur la légitimité de la police ou d'autres autorités qui vous arrêtent en cours de route :
 - Appelez la police pour confirmer la légitimité de l'arrêt et informez-les de vos préoccupations.
 - Informez toujours votre centre de répartition/surveillance lorsqu'une autorité sur la route vous demande d'arrêter votre véhicule.
 - Demandez aux autorités de vous accompagner jusqu'au poste de police le plus proche pour les vérifications nécessaires tout en gardant votre centre de répartition/surveillance informé.
- Installez une serrure de haute sécurité pour éviter l'ouverture des portes du compartiment de chargement pendant la conduite.
- Installez des capteurs pour vous informer lorsque les portes arrière sont ouvertes en cours de route.

Ne pas faire :

- Ne faites pas aveuglément confiance aux individus prétendant être des policiers ou d'autres autorités sans vérifier leurs références ou leur identification.
- Ne déviez pas de votre itinéraire planifié ou ne changez pas de lieux de livraison sans confirmation de votre centre de répartition/surveillance.
- N'hésitez pas à signaler tout incident suspect ou toute préoccupation à la police, à votre centre de répartition/surveillance et aux autorités compétentes.

Comment signaler une menace de tromperie ?

Si vous êtes arrêté par la police ou d'autres autorités pour des vérifications, contactez immédiatement votre centre de répartition ou de surveillance et fournissez des informations sur :

-  Votre emplacement.
-  Le type d'autorités (si possible).
-  La plaque d'immatriculation du véhicule ou d'autres caractéristiques des autorités.

Détournement

Quelle est la menace de détournement ?

Le détournement consiste à voler (des marchandises) d'un camion ou d'un autre véhicule après l'avoir forcé à s'arrêter, par exemple détourner une cargaison de tabac. Cela signifie également voler un véhicule après l'avoir forcé à s'arrêter, souvent sans violence. Les incidents de détournement présentent un risque important pour les conducteurs, avec la possibilité de blessures graves, voire de décès.



TAPA EMEA[®]
Transported Asset Protection Association

Thorsten Neumann highlighted three extreme contributors to the data presented for the first three-quarters of the year. These included €300 million of losses recorded in just two crimes; one involving the hijacking of miscellaneous goods in Belgium, and the other a case of fraud detected within a metal supply chain by a global organisation based in Germany.

Comment prévenir la menace de détournement ?

- **Soyez attentif pendant la conduite**
Comme indiqué dans la définition, dans les situations de détournement, le camion doit s'arrêter pour que les criminels prennent le contrôle de celui-ci. Par conséquent, la manière la plus importante d'éviter les situations de détournement est de ne pas s'arrêter lorsque ces situations sont évidentes et imminentes. Par exemple, si des individus qui ne semblent pas être des autorités légitimes vous demandent de vous arrêter sur la route, il est important de faire preuve de prudence et de privilégier votre sécurité. Même des individus se faisant passer pour de faux policiers ou d'autres autorités peuvent représenter un risque.
- **Reconnaissance des menaces émergentes**
Il est crucial d'être vigilant et préparé à gérer des situations hostiles. Généralement, les preneurs d'otages vous suivent avant de tenter de prendre le contrôle du véhicule ou conduisent devant vous à une vitesse constante pour surveiller votre comportement au volant.

Comment répondre à la menace de détournement ?

À faire :

- Gardez toutes les portes et fenêtres verrouillées pendant la conduite.
- Restez vigilant et soyez conscient de votre environnement. Faites attention à toute activité, véhicule ou individu suspect ou inhabituel.
- Essayez de créer de la distance entre votre véhicule et le véhicule suspect, afin que, en cas d'arrêt, vous puissiez manoeuvrer et vous éloigner.
- Maintenez un contact régulier avec votre centre de répartition/surveillance ou d'autres contacts désignés et partagez avec eux des mises à jour sur votre emplacement et toute déviation par rapport à l'itinéraire prévu.

À ne pas faire :

- Ne permettez à personne de monter dans votre cabine.
- Ne vous arrêtez pas et ne sortez pas du véhicule à moins d'avoir confirmé la validité des autorités qui vous ont demandé de le faire.
- Ne résistez pas ou ne confrontez pas les preneurs d'otages.
- Ne faites pas de mouvements brusques ou suspects.
- Ne fournissez pas d'informations inutiles aux preneurs d'otages.

Comment signaler une menace de détournement ?

Après un incident de détournement, il est crucial de signaler l'incident à la police et à votre centre de répartition/surveillance dès que cela est possible en toute sécurité. Fournissez-leur tous les détails pertinents pour aider à

- 📍 Date/heure/lieu de l'incident et votre emplacement actuel (si différent du lieu de l'incident).
- 🕒 Toute blessure ou besoin de soutien médical d'urgence.
- 🕒 Nom du conducteur/plaques d'immatriculation du camion/remorque.
- 👥 Nombre de criminels impliqués.
- 👮 Type d'autorités (si possible).
- 🚗 Toute plaque d'immatriculation de véhicule ou autres caractéristiques des autorités.

L'entrée d'immigrants illégaux

Quelle est la menace d'entrée d'immigrants illégaux ?

La menace d'entrée d'immigrants illégaux fait référence au problème des personnes non autorisées tentant d'entrer dans les pays en se cachant dans des véhicules de fret routier. Alors que la migration illégale se produit à l'échelle mondiale à travers divers modes de transport, la crise des migrants en Europe a particulièrement impacté le transport terrestre, notamment le transport routier et ferroviaire de marchandises.

Les réseaux criminels impliqués dans le trafic de migrants représentent une menace significative, certains réseaux se concentrant uniquement sur la facilitation de passages frontaliers illégaux à travers des véhicules de fret routier. Cela pose de nombreux défis et risques pour les entreprises de transport routier de marchandises. Certaines des conséquences comprennent des dommages matériels et de cargaison, des violences physiques et psychologiques contre les conducteurs, et d'autres problèmes connexes. De plus, dans les cas où la cargaison est constituée de produits pharmaceutiques ou alimentaires, toute intrusion d'immigrants illégaux dans le compartiment de chargement ou l'ouverture partielle des emballages est considérée comme une contamination, et la cargaison est rejetée pour la livraison.

Actuellement, les débats sur les problèmes causés par les immigrants illégaux aux entreprises de transport routier de marchandises européennes ne sont pas largement abordés.

Case example

CRIMINAL NETWORK CHARGING UP TO EUR 20 000 PER MIGRANT

A criminal network facilitates the entry and secondary movements of irregular migrants in the EU. Migrants pay enormous sums to the smugglers to enter the EU clandestinely and move on to further destinations within its borders. The entire journey from the country of origin to the EU costs between EUR 15 000 and 20 000. The criminals advertise their illicit activities on various social media platforms to lure migrants, also by posting videos of successful transports. Migrants are moved along two main routes, either from Croatia via Slovenia to Italy, or from Serbia via Hungary to Austria.²⁵

Comment prévenir la menace d'entrée d'immigrants illégaux ?

Vérifications des véhicules avant et après chaque arrêt.

Il est courant que les immigrants illégaux tentent de pénétrer dans un véhicule lorsqu'il est arrêté ou stationné. Pour prévenir cela, il est fortement recommandé d'effectuer des vérifications des véhicules avant et après chaque arrêt. Cette pratique consiste à faire le tour du véhicule et à s'assurer qu'il n'y a aucun signe de tentative d'entrée dans le compartiment de chargement, à vérifier l'intégrité des scellés et à confirmer que toutes les portes, serrures et fermetures sont correctement fermées et sécurisées.



Comment répondre à la menace d'entrée d'immigrants illégaux ?

À faire :

- Être présent lorsque votre camion est chargé.
- Les scellés et les serrures/cadenas sont verrouillés/fixés correctement immédiatement après le chargement.
- Lorsque vous prenez la responsabilité du véhicule, vous devez vous assurer qu'il ne contient pas de personnes non autorisées.
- Vérifiez votre véhicule et votre remorque pour détecter toute irrégularité avant de poursuivre votre voyage. Les scellés, les serrures, les portes et la bâche sont en bon état et n'ont pas été manipulés.
- Vérifiez toujours périphériquement votre véhicule après une pause courte ou longue pour confirmer l'absence de signes d'intrusion et que les scellés et les serrures sont intacts.
- Vérifiez tous les compartiments de rangement externes, les essieux, les boîtes à outils, les déflecteurs de vent et le dessous du véhicule.

À ne pas faire :

- **NE PAS** utiliser des emplacements de stationnement non classés pour des pauses courtes et longues dans des zones où le risque d'entrée d'immigrants illégaux dans votre véhicule est élevé.
- **NE PLANIFIEZ PAS** une pause / un séjour d'une nuit dans des zones éloignées (par exemple, zones industrielles, aires de repos).
- **NE FAITES PAS** d'arrêts inutiles pendant la conduite, surtout s'il n'y a pas d'arrêts prévus ou d'urgences.
- **NE VOUS ARRÊTEZ PAS** immédiatement si d'autres personnes vous signalent de le faire (par exemple, pour un "problème" avec votre véhicule).
- **NE PAS** ouvrir la remorque/le véhicule.
- **NE PAS** approcher les clandestins, maintenez une distance.
- **NE TOUCHEZ PAS** la cargaison/la remorque, car il y a un risque de contamination.

Comment signaler la menace d'entrée d'immigrants illégaux ?

Si vous êtes témoin ou soupçonnez une menace d'entrée d'immigrants illégaux, contactez immédiatement les forces de l'ordre locales ou les services d'urgence de votre région.



Fournissez-leur tous les détails pertinents, notamment :

- la localisation
- le nombre de personnes impliquées
- toute information d'identification sur les personnes impliquées



Informez votre centre de répartition/surveillance ou le personnel approprié au sein de votre entreprise de la menace d'entrée d'immigrants illégaux.



Suivez les procédures de votre entreprise.

Criminalité des véhicules de la dernière mile

Quelle est la menace de la criminalité des véhicules de la dernière mile ?

La menace de la criminalité des véhicules de la dernière mile désigne les activités criminelles qui ciblent généralement les véhicules utilisés pour la livraison de la dernière mile dans les zones urbaines. Ces véhicules, tels que les minifourgonnettes ou les petits camions à caisse, font souvent plusieurs arrêts pour livrer ou récupérer de petits colis. Les véhicules de la dernière mile sont particulièrement vulnérables à ces types de crimes en raison des arrêts fréquents et du contenu de valeur qu'ils transportent.

Comment prévenir la menace de la criminalité des véhicules de la dernière mile ?

- Systèmes de sécurité adaptés aux véhicules (verrouillage automatique, bracelets RFID, etc.)
Il existe de nombreux systèmes de sécurité adaptés pour prévenir ce type d'incidents, mais la mesure la plus importante est de toujours verrouiller toutes les portes des véhicules et d'activer les systèmes de sécurité installés (alarme d'intrusion, dispositif d'immobilisation, etc.).

Il existe des systèmes de sécurité très avancés disponibles récemment (par exemple, des bracelets RFID au poignet du conducteur qui verrouillent automatiquement les portes du véhicule et activent tous les systèmes de sécurité lorsque le conducteur s'éloigne à une certaine distance du véhicule (c'est-à-dire 3 à 5 mètres). Ces bracelets déverrouillent également les serrures du véhicule lorsque le conducteur atteint une distance spécifique par rapport à celui-ci.

Comment répondre à la menace de la criminalité des véhicules de la dernière mile ?

À faire :

- Toujours verrouiller votre véhicule et activer tous les systèmes de sécurité lorsque vous vous arrêtez pour effectuer une livraison.
- Soyez vigilant et conscient de votre environnement.
- Identifier les comportements ou individus suspects et signaler tout incident inhabituel à votre centre de surveillance / dispatching.
- Transporter une télécommande pour activer la sirène du système d'alarme du véhicule en cas de visualisation à distance que quelqu'un soit entré dans votre véhicule ou tente d'y entrer.

Ne pas faire :

- **NE PAS** stationner loin du point de livraison et devoir marcher sur une longue distance avec les colis à la main pour atteindre le point de livraison.
- **NE PAS** vous surcharger de colis en sortant de votre véhicule pour effectuer la livraison, de sorte que vos mains soient occupées et que vous essayiez de fermer les portes du véhicule avec votre jambe.
- **NE PAS** laisser vos clés sur le contact ou sans surveillance à l'intérieur du véhicule, même pour une courte période.
- **NE PAS** laisser d'objets de valeur, y compris des effets personnels ou des colis de grande valeur, visibles de l'extérieur du véhicule.
- **NE PAS** partager des informations de livraison spécifiques, telles que le contenu exact, les adresses ou les horaires de livraison, avec des personnes non autorisées ou non impliquées dans le processus de livraison.

Comment signaler la menace de crime liée aux véhicules de dernière mile ?

Signaler une menace ou un incident de criminalité des véhicules de dernière mile est crucial pour faire face à la situation et garantir votre sécurité, celle de votre véhicule et des colis en cours de livraison. Voici comment vous pouvez signaler de tels incidents :

-  Signalez immédiatement l'incident à l'agence locale de maintien de l'ordre ou aux services d'urgence de votre région.
-  Fournissez-leur tous les détails pertinents, y compris l'emplacement, la description de l'incident et toute information d'identification sur les personnes impliquées.
-  Signalez la menace de criminalité des véhicules de dernière mile à votre centre de répartition/surveillance ou au personnel approprié au sein de votre entreprise.
-  Essayez de préserver toute preuve liée à l'incident, comme des photographies, des vidéos ou toute preuve matérielle pouvant être utile pour l'enquête.

Cybercriminalité et fuite de sécurité des informations

Quelle est la menace de cybercriminalité et de fuite de sécurité des informations ? En matière de sécurité de la chaîne d'approvisionnement, lorsque nous parlons de cybercriminalité, nous faisons référence à une attaque visant les systèmes d'information dans le but de voler des informations sensibles sur les marchandises (par exemple, origine et destination des itinéraires, types et valeurs des marchandises) ou à une fuite d'informations involontaire par les fournisseurs de services logistiques ou les conducteurs. Dans ce document, nous nous concentrerons sur la fuite involontaire d'informations par les conducteurs via leurs comptes de médias sociaux ou leurs comptes de messagerie électronique.

Comment prévenir la menace de cybercriminalité et de fuite de sécurité des informations ?

Il nécessite des mesures de défense solides, en comprenant que la supervision humaine reste le maillon le plus faible. Les criminels exploitent souvent les vulnérabilités à travers des e-mails d'hameçonnage, des fichiers de documents malveillants, des techniques d'ingénierie sociale et des logiciels et matériels non mis à jour.

- Soyez vigilant pour les attaques de phishing sur les téléphones et tablettes

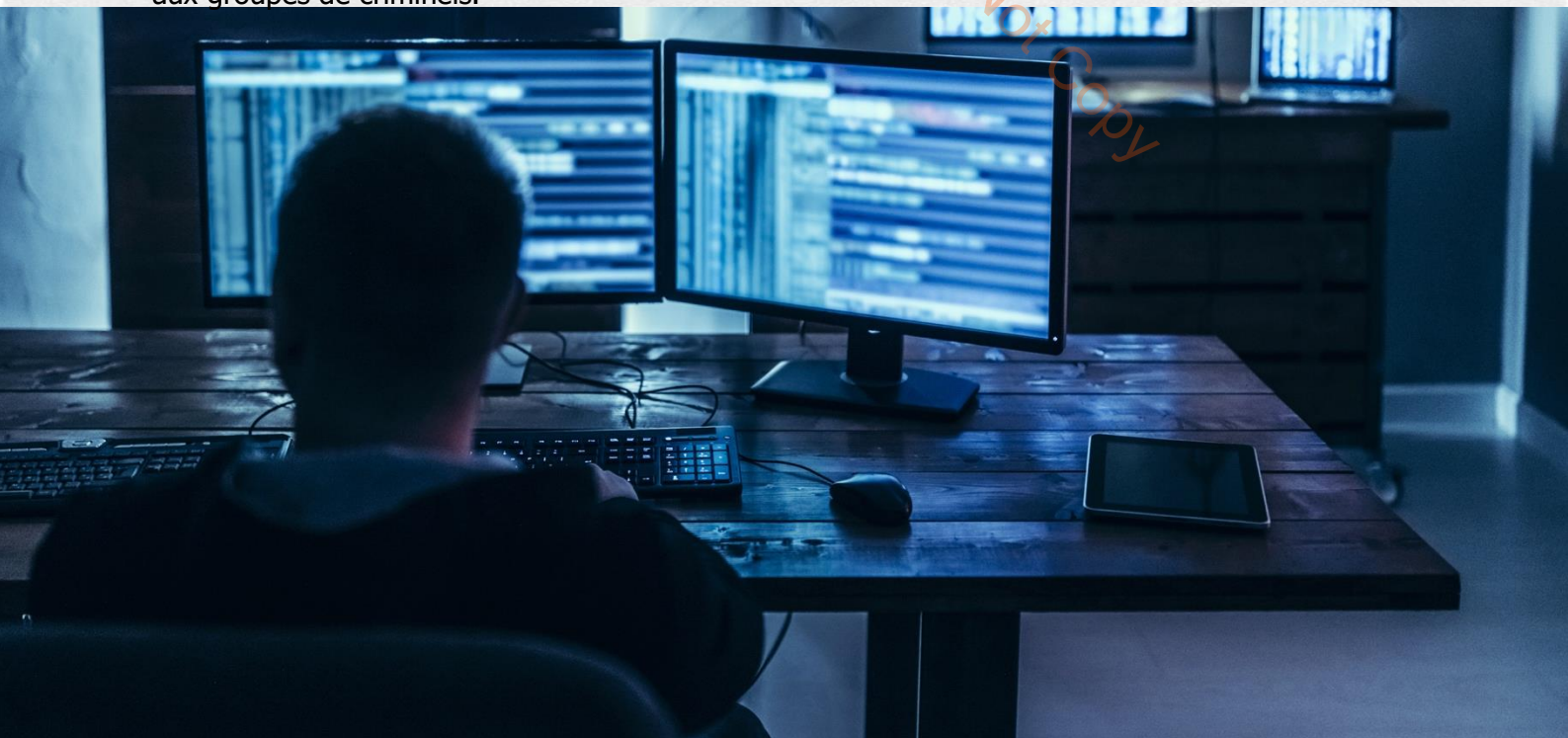
Vous devriez toujours valider les e-mails entrants, surtout ceux qui vous demandent d'utiliser un lien pour aller plus loin. De cette manière, les criminels peuvent accéder aux informations stockées sur votre téléphone, y compris les détails des itinéraires et des cargaisons.

- Protection des informations d'expédition et des documents

Les criminels peuvent efficacement organiser une attaque en ayant accès aux documents d'expédition, qui contiennent des informations vitales. Par exemple, un document CMR comprend des détails tels que l'origine, la destination, le type, la quantité, le nom du conducteur, le numéro de scellé, et plus encore. Si les criminels ciblent votre cargaison, avoir accès à ces informations leur suffit pour commencer à organiser l'attaque.

- Besoin de savoir sur une base d'informations

Les documents d'expédition ne sont pas le seul moyen pour les criminels d'obtenir accès à ces informations. Souvent, la distribution non contrôlée de ces informations (verbalement ou par écrit) parmi les employés, en particulier ceux qui ne devraient pas connaître ces informations, est suffisante pour qu'une personne correctement formée puisse extraire ces informations et les fournir aux groupes de criminels.



Comment répondre à la menace de cybercriminalité et de fuite de sécurité des informations ?

Si vous soupçonnez une fuite d'informations, que ce soit à partir de systèmes informatiques ou de documents non contrôlés, vous devez signaler cela à votre centre de dispatching et leur demander des instructions sur la manière d'atténuer ses conséquences.

Comment répondre à la menace de cybercriminalité et de fuite de sécurité des informations ?

À faire :

- Vérifiez toujours les détails de l'expéditeur avant de cliquer sur un lien dans un e-mail reçu.
- Protégez les documents d'expédition pendant qu'ils sont sous votre garde.
- Signalez tout comportement inhabituel de votre téléphone portable et demandez à votre service informatique de le vérifier.
- Signalez toute activité ou incident suspect à votre service informatique ou à l'équipe de sécurité de votre organisation.
- Utilisez des mots de passe forts et uniques pour tous vos comptes et l'accès au téléphone portable.

Ne pas faire :

- **NE PAS** répondre aux appels entrants provenant de numéros inconnus (généralement de l'étranger).
- **NE PAS** partager d'informations sur vos itinéraires, y compris le type de cargaison, la valeur estimée, l'origine, la destination et les arrêts de repos, avec des personnes qui n'ont pas besoin de ces informations.
- **NE PAS** publier d'informations liées à votre travail et des photos sur les réseaux sociaux.
- **NE PAS** laisser vos appareils sans surveillance ou déverrouillés, surtout dans les lieux publics.

Comment signaler une menace de cybercriminalité et de fuite de sécurité des informations ?

Si vous soupçonnez d'être victime d'une cybercriminalité liée à votre itinéraire de transport ou si vous avez remarqué une fuite de détails de votre itinéraire, signalez-le immédiatement à votre répartiteur/superviseur. Dans votre rapport, incluez les détails suivants :

-  Comment vous avez identifié la fuite ou soupçonné une cybercriminalité.
-  Quelles informations spécifiques ont été divulguées ou compromises.

Fonctionnalités et soutien des centres de dispatching ou de surveillance et de réponse aux conducteurs

Les centres de surveillance et de réponse jouent un rôle crucial dans la sécurité des actifs, tels que les camions ou les remorques, pendant le transport. Il est important de comprendre la distinction entre le suivi et la surveillance :

- Suivi: Le suivi consiste à connaître le statut ou la localisation de votre camion et/ou remorque. Il fournit des informations en temps réel sur l'emplacement du véhicule, permettant ainsi une visibilité et un suivi de ses mouvements.
- Surveillance: La surveillance va au-delà du suivi en comparant le statut réel de votre camion et/ou remorque, tel que sa localisation, avec le statut planifié ou attendu. Cela implique d'avoir un plan ou un itinéraire prédéfini et de comparer en continu les données réelles fournies par le système de suivi avec les données attendues.

Il est important de noter que la surveillance ne peut avoir lieu que lorsqu'il existe un plan ou un itinéraire prédéfini. Sans une planification adéquate, il n'y a rien à surveiller. Par conséquent, les centres de surveillance s'appuient sur une planification précise et des informations de suivi en temps réel pour surveiller efficacement la progression et la sécurité des actifs pendant le transport.

Veuillez noter que même dans les transports où il n'y a pas de fonction de surveillance dédiée pour superviser l'exécution de l'itinéraire, il y a toujours une sorte de supervision de la part des planificateurs de transport envers les conducteurs et les marchandises pour s'assurer qu'il n'y a pas d'événements inattendus pendant le transport. Par conséquent, considérez toujours qu'il y a quelqu'un au bureau central ou au centre de surveillance qui veille sur votre sécurité et la sécurité de votre cargaison.

L'itinéraire est une combinaison de :

- un camion (avec la remorque, le cas échéant),
- un conducteur,
- une origine,
- une destination,
- une heure de départ,
- une heure d'arrivée estimée, et
- des arrêts planifiés à des emplacements prédéfinis avec des intervalles de temps associés pour chaque arrêt entre ceux-ci.



Il existe plusieurs techniques / modes de surveillance :

- **Surveillance active** : La station de surveillance suit et surveille activement l'emplacement et la progression de l'actif tout au long de la durée de l'itinéraire en temps réel.
- **Surveillance passive** : La station de surveillance vérifie et enregistre l'exécution de l'itinéraire une fois, ou quelques fois pendant sa durée.
- **Surveillance par exception** : La station de surveillance reçoit des alarmes ou des notifications uniquement en cas d'écart par rapport à l'itinéraire ou à l'horaire prévu.
- **Surveillance par intervalle de temps** : La station de surveillance vérifie l'exécution de l'itinéraire à des intervalles de temps réguliers, comme toutes les 15, 30 ou 60 minutes. Elle vérifie si l'actif suit l'itinéraire prévu et respecte l'horaire attendu dans ces intervalles prédéfinis.
- **Surveillance par étape de l'itinéraire** : La station de surveillance vérifie chaque étape spécifique (c'est-à-dire l'arrivée à un emplacement spécifique) pour s'assurer que l'itinéraire est exécuté conformément au plan.

En principe, la responsabilité d'une station de surveillance est de :

- Recevoir,
- Vérifier, et
- Répondre à un événement d'alarme (toute déviation par rapport à l'itinéraire prévu) dans un intervalle de temps convenu.

La vérification est généralement effectuée par communication téléphonique entre la station de surveillance et le conducteur, en utilisant un mot-clé spécifique. Le conducteur doit inclure le mot-clé dans sa réponse pour s'identifier et confirmer son statut. Cependant, sur les routes à haut risque, le conducteur peut être instruit d'exclure le mot-clé en cas d'alarme réelle, telle qu'une prise d'otage. Lorsque le conducteur peut communiquer avec la station de surveillance, il est crucial pour lui de fournir des informations précises. Cela permet à l'opérateur de la station de surveillance de comprendre pleinement la situation et d'initier le protocole de réponse approprié.

Dans le cas où un conducteur serait sous une prise d'otage, des protocoles de réponse prédéfinis doivent être en place. Ces protocoles tiennent compte du fait que le conducteur pourrait ne pas être en mesure de fournir une description précise de la situation en raison des circonstances hostiles. La station de surveillance initiera les actions de réponse nécessaires en fonction des protocoles établis pour assurer la sécurité du conducteur et du chargement.

European Emergency Contact Numbers

Country	Police	Emergency/Ambulance Services
Austria	133 or +43 59 133	112
Belgium	101	112
Bulgaria	112 or 166 or 02 98 28 363	112 or 160
Croatia	112 or 192	112 or 194
Cyprus	112 or 199	112 or 199
Czech Republic	112 or 158	112 or 155
Denmark	112 or 114	112
Estonia	112	112
Finland	112	112
France	17 or 112	15 or 112
Germany	110	112
Greece	100 or 112	166 or 112
Hungary	107 or 112	104 or 112
Ireland	112 or 999	112 or 999
Italy	112 or 113	112 or 118
Latvia	110 or 112	113 or 112
Lithuania	112	112
Luxembourg	113	112
Malta	112	112
Netherlands	112	112
Poland	112 or 997	112 or 999
Portugal	112	112
Romania	112	112
Spain	112 or 091 or 092	112 or 061
Slovakia	112	112 or 155
Slovenia	112 or 113	112
Sweden	112	112
Switzerland	117	144
UK	999	999 or 111



Règles précieuses pour les conducteurs

Vous transportez des marchandises qui pourraient être ciblées par des criminels organisés ou opportunistes. Pour vous protéger ainsi que votre fret, suivez les instructions ci-dessous sans exception :

1. Utilisez les autoroutes pour les trajets longue distance vers les destinations principales. Si possible, évitez d'emprunter les routes secondaires et les raccourcis.
2. Les conducteurs et les assistants ne doivent pas communiquer, discuter et/ou divulguer des informations concernant leur cargaison à d'autres parties ou personnes pendant leur trajet vers leur destination. La divulgation d'informations professionnelles (itinéraires, cargaison, etc.) sur les comptes de médias sociaux personnels doit également être évitée.
3. Ne transportez jamais de passagers non autorisés. Ne prenez jamais d'auto-stoppeur.
4. Gardez toujours votre véhicule sécurisé, même lorsque vous conduisez.
5. Ne laissez jamais le véhicule ou la cargaison sans surveillance à aucun moment. Les pauses confort (comme les repas et/ou les pauses toilettes) ne doivent pas déroger à ce processus – si deux conducteurs sont à bord, l'un d'eux doit rester avec le véhicule en tout temps. Si le véhicule doit s'arrêter pour une période prolongée, vérifiez auprès du centre de répartition ou de surveillance pour vous assurer de ne vous garer que dans des endroits sécurisés approuvés, tels que des aires de stationnement certifiées, des postes de péage ou des postes de police dans les petites villes ou villages. Voyagez en convois lorsque c'est possible.
6. Si vous devez vous garer à l'extérieur d'une zone sécurisée/protégée, prenez des mesures de sécurité supplémentaires, comme garer le véhicule avec les portes arrière contre un autre camion ou contre un mur.
7. Si la livraison ne peut pas être effectuée, il faut demander des conseils à la base ou au centre de surveillance sur ce qu'il faut faire avec la cargaison.
8. Insistez toujours sur des signatures de POD claires et précises. Le chauffeur doit vérifier l'identité de la personne acceptant les marchandises au nom du client avant de remettre les colis. Remettez en question tout changement de dernière minute.
9. Traitez les offres d'assistance non sollicitées de la part de personnes inconnues avec prudence.
10. Traitez avec une extrême prudence les signaux d'autres conducteurs indiquant qu'il y a un problème avec votre véhicule.
11. Parfois, les criminels se font passer pour des policiers ou d'autres fonctionnaires gouvernementaux ; par conséquent, une attention supplémentaire doit être accordée lorsque les conducteurs sont confrontés de manière inattendue à des responsables. Les conducteurs doivent informer leur centre de répartition ou de surveillance de leur emplacement avant de s'arrêter si cela est sûr à faire.
12. Maintenez un contact régulier avec le centre de répartition/base. Le conducteur doit disposer de plusieurs méthodes pour contacter le centre de répartition/base (par exemple, le télex, le téléphone portable, la radio RF, etc.). Le conducteur doit toujours porter un téléphone portable ou tout autre dispositif de communication.
13. Surveillez vos rétroviseurs et prenez note de tout véhicule qui pourrait suivre votre camion. Signalez tout véhicule ou incident suspect sur-le-champ.
14. Possédez une carte d'information sur la sécurité du conducteur comprenant tous les numéros de contact d'urgence.
15. Soyez vigilant lorsque vous acceptez des appels ou des e-mails entrants provenant de numéros ou de comptes inconnus.

Ne jamais enfreindre les règles. Ces règles sont la base pour prendre en charge le fret et effectuer le transport !

References

1. European Parliament study on Organized Theft of Commercial Vehicles and their Loads in the European Union
2. International Journal of Retail & Distribution Management Vol. 43 No. 3, 2015 pp. 204-220, Cargo Theft at non-secure parking locations, ©Emerald Group Publishing Limited, 0959-0552, DOI 10.1108/IJRDM-06-2013-0131
3. TAPA EMEA, 18 MONTHS OF CARGO CRIME EUROPE, MIDDLE EAST & AFRICA REGION, REPORTING PERIOD TO 30 JUNE 2022
4. The International Journal ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES ISSN 2345-0282, 2018 Volume 5 Number 3 (March) PECULIARITIES OF ILLEGAL IMMIGRANT'S INTRUSIONS INTO ROAD FREIGHT TRANSPORT UNITS IN THE FRANCE - UK CORRIDOR
5. Europol DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS, PDF | ISBN 978-92-95236-25-7 | DOI: 10.2813/811566 | QL-05-24-250-EN-N
6. Cyber-Security and Information Warfare, Copyright © 2019 by Nova Science Publishers, Inc. pp. 201, A Case Study Analysis of Attacks and Losses in the Supply Chain with the Use of GPS or GSM Jammers by the Attackers Panayiotis Laimos, Michalis Chronopoulos, Chrysanthi Laimou and Nikoleta Atanasova, ISBN: 978-1-53614-386-7
7. <https://www.fleeteurope.com/en/technology-and-innovation/global/features/ransomware-rise-again-causing-shattering-damages-fleets?t%5B0%5D=Fleet%20Management&curl=1>
8. Europol Internet Organised Crime Threat Assessment (IOCTA) 2023, Luxembourg: Publications Office of the European Union, 2023, PDF ISBN: 978-92-95220-83-6 ISSN: 2363-1627 doi:10.2813/587536 QL-AL-23-001-EN-N, © European Union Agency for Law Enforcement Cooperation, 2023
9. <https://www.cybertalk.org/2021/07/28/ransomware-attacks-on-the-transportation-industry-2021/> Ransomware attacks on the transportation industry, 2021
10. <https://www.telegraph.co.uk/news/uknews/immigration/11694134/Calais-crisis-Illegal-immigrants-shut-down-all-Channel-traffic.html>
11. BSI and TT Club 2023 Cargo Theft Report, April 2024

Clause de non-responsabilité pour le Guide de sécurité du conducteur

Ce document de conseils en sécurité pour les conducteurs fournit des astuces utiles et des informations compilées au mieux de nos connaissances et de notre croyance, sur la base de l'expérience et des informations de base. Les sujets ont été sélectionnés en fonction des tendances actuelles et des besoins en 2024, élucidés et publiés par TAPA EMEA. L'association agit en tant que soutien de l'industrie et de la chaîne d'approvisionnement connexe dans ce contexte, dans le but de minimiser la possibilité de pertes liées aux risques mentionnés dans le présent document.

Veuillez noter que le nombre et la liste des points mentionnés peuvent ne pas être exhaustifs, et tous les dangers potentiels ou autres risques dangereux ne sont pas nécessairement répertoriés ici.

Les recommandations concernant les actions à éviter ou les comportements appropriés mentionnés dans le document reflètent également l'expertise des experts de TAPA EMEA impliqués dans la création du présent Guide de sécurité des conducteurs.

Ce document sert uniquement de support et de mesure de sensibilisation pour les conducteurs de marchandises générales et de HVC. La responsabilité de sa mise en œuvre, de son utilisation appropriée et de son application correcte incombe au lecteur, à l'utilisateur ou à l'industrie, y compris les prestataires de services logistiques.

L'utilisateur/lecteur du document/politique est conscient des actions associées. Ni TAPA EMEA ni les experts contributeurs n'assument aucune obligation, responsabilité ou responsabilité délictuelle concernant les sujets mentionnés ici, leur traitement ou les données fournies, qui reposent sur la confiance dans les références mentionnées et fournies par des tiers.

Informations de publication et de droits d'auteur

La mention de copyright de TAPA EMEA affichée dans ce document indique la date de sa dernière publication.

@ TAPA EMEA 2024

Aucun droit d'auteur sans autorisation de TAPA EMEA, sauf dans les cas permis par la loi sur le copyright.

Historique de publication

Première publication en juin 2024.

La présente édition a été publiée en juin 2024.

