

Table des matières

A - LA SÉCURITÉ CHEZ SOI

I - « PENSONS SÉCURITÉ »

II - ET SI.....

III -LORSQUE VOUS QUITTEZ LA MAISON

B - LA SÉCURITÉ DANS LA RUE

I -Dans la rue, si vous vous rendez à pied ou trouvez dans un endroit que vous estimez peu sûr, il existe des moyens de réduire les risques et d'accroître votre sentiment de sécurité.

II -Les automobilistes: Il existe quelques règles élémentaires à suivre dans certaines situations. Sachez faire preuve de jugement afin de décider des mesures à prendre.

III - Les vols de téléphones portables: Il existe des actes réflexes pour s'en protéger.

C - LA SÉCURITÉ SUR INTERNET

INFORMATION DESTINÉE AUX PARENTS

INFORMATION DESTINÉE AUX ADOLESCENTS

D - LA SÉCURITÉ INFORMATIQUE DANS L'ENTREPRISE

E - LA SÉCURITÉ DES COMMERÇANTS

LA SÉCURITÉ CHEZ SOI

Introduction

Ensemble, nous pouvons bâtir un environnement plus sûr. L'éducation et la sensibilisation aux techniques de prévention situationnelle peuvent vous aider à reconnaître les situations dangereuses et vous permettre de prendre des mesures simples dans le but de réduire ou d'éliminer les risques.

I - « PENSONS SÉCURITÉ »

De nombreuses personnes négligent de prendre dans leur habitation des mesures élémentaires afin de se prémunir contre le vol. Pourtant, en prenant librement certaines précautions, vous réduirez les risques.

Gardez si nécessaire une ou deux entrées et le garage éclairés la nuit (lampes faible intensité).

Ne laissez pas de signes évidents de votre absence même momentanée.

Installez de bonnes serrures et utilisez-les toujours, y compris lorsque vous êtes chez vous. Ne laissez pas inutilement de fenêtre ouverte, notamment au rez-de-chaussée. N'inscrivez pas vos nom et adresse sur votre porte-clés; ne laissez pas vos clés sous un paillason ou dans la boîte aux lettres.

Installez sur la porte un microviseur à grand champ de vision qui permet de voir les visiteurs avant d'ouvrir; ou un entrebâilleur.

N'ouvrez jamais la porte à des étrangers sans preuve d'identité. Méfiez-vous des usurpateurs d'identité, et n'hésitez pas à demander des cartes professionnelles ou documents officiels aux personnels d'EDF-GDF, de la Poste, de France Télécom, des forces de l'ordre... que vous ne connaissez pas, qui ne vous inspirent pas confiance et qui se présentent chez vous sans préavis.

Changez vos habitudes. Les cambrioleurs s'y fient!

Ne gardez pas d'importantes sommes d'argent chez vous.

Identifiez les objets de valeur (bijoux, appareils hi-fi, meubles anciens...). Gardez factures (avec n° de série pour appareils hi-fi) et photographies qui seront utiles aux enquêteurs en cas de vol. En effet, ces photos ou n° de série seront inscrits dans une base d'objets volés, facilitant ainsi les recherches.

Conservez les objets de grande valeur à la banque, dans un coffret de sûreté. Si cette solution n'est pas pratique, gardez-les sous clé dans un endroit de la maison sûr, caché et connu de vous seul.

Globalement soyez vigilants avec les démarcheurs à domicile, notamment si vous êtes seul. Évitez si possible de les recevoir seul. Ne vous laissez pas abuser en signant un papier qui ne vous semble pas clair, car en matière de démarchage vous disposez toujours d'un délai de réflexion.

II - ET SI.....

Un cambrioleur s'introduit dans votre habitation alors que vous êtes présent.

Mettez-le en fuite en criant; mais, sauf s'il vous agresse physiquement, évitez d'attaquer cet individu qui sera probablement aussi effrayé. En outre, il est rappelé que la défense légitime et proportionnée de vos biens en cas de crime ou délit, prévue par la loi, ne permet jamais l'homicide du cambrioleur.

Essayez de noter son allure, son signalement précis (âge apparent, taille, corpulence, couleur de peau, couleur des yeux, couleur/coupe de cheveux, signes particuliers, tatouages, tenue vestimentaire, tics, accent, gaucher/droitier...). Si vous le pouvez, relevez les caractéristiques du véhicule qu'il utilise (couleur, type, marque, immatriculation, direction de fuite, points particuliers).

Appelez dès que vous le pouvez la gendarmerie ou la police.

LE VRAI ET LE FAUX

On a tort de s'imaginer le cambrioleur comme étant toujours un visiteur nocturne, qui porte un masque, un imperméable avec collet relevé et une casquette.

Dans certains cas, il est bien vêtu ou porte un habit quelconque. Son âge est très variable.

Le vol peut avoir lieu en plein jour, souvent de 9h00 à 17h00, lorsque les habitants du lieu sont au travail.

Le cambrioleur ne vous veut souvent aucun mal. Il désire simplement pénétrer dans votre demeure (parfois même lorsque vous êtes présent), faire main basse sur les articles de valeur et déguerpir sans être vu.

III -LORSQUE VOUS QUITTEZ LA MAISON

Il est important de bien protéger votre demeure lorsque vous vous absentez pour un certain temps. Votre maison doit non seulement être verrouillée, mais elle doit aussi paraître habitée.

Avant de partir, verrouillez toutes les portes, y compris de garage ou jardin, fenêtres et volets. Branchez votre alarme si vous en disposez.

Pour les absences de courte durée, laissez une ou deux lampes allumées, de préférence raccordées à une minuterie qui les allume par intermittence lorsque la nuit vient.

Demandez à quelqu'un de ramasser le courrier ou les journaux laissés à votre porte.

Laissez votre clé uniquement à une personne de confiance. Vous lui demanderez de venir parfois de jour ouvrir quelques heures les volets pour donner l'illusion que votre logement est habité.

Mentionnez à vos voisins de confiance ou au gardien d'immeuble que vous serez absent durant un certain temps et précisez les dates de départ et de retour ainsi que le numéro de téléphone où l'on peut vous rejoindre en cas d'urgence.

N'indiquez jamais sur le message de votre répondeur que vous serez absent; transférez vos appels.

En cas de cambriolage, surtout ne touchez à rien et appelez la gendarmerie ! Il faut préserver les éventuelles traces et empreintes qui pourront être exploitées par la police technique et scientifique.

De manière générale, n'oubliez pas que parmi vos voisins, il peut y avoir un élu, un gendarme, un réserviste / retraité de la gendarmerie, un policier national ou municipal, un pompier, un douanier, un gardien d'immeuble, un responsable d'association de quartier..., en qui vous pouvez avoir confiance, et ainsi signaler tout fait suspect (p.ex. véhicule louche aperçu). Cette personne, si vous le préférez, pourra se charger, en fonction des éléments recueillis, d'avertir la gendarmerie. Elle structurera naturellement les solidarités de voisinage, dynamisera la vigilance citoyenne, le civisme du quotidien.

LA SÉCURITÉ DANS LA RUE

I -Dans la rue, si vous vous rendez à pied ou trouvez dans un endroit que vous estimez peu sûr, il existe des moyens de réduire les risques et d'accroître votre sentiment de sécurité.

De nuit, marchez de préférence dans les endroits éclairés.

Si possible, ne vous encombrez pas de gros paquets; préférez le sac en bandoulière au sac à main et tenez-le du côté opposé à la chaussée pour éviter le vol à la tire. Bannissez les objets de valeur dans un sac à dos qui faciliterait le travail des "pickpockets".

N'étalez jamais d'importantes sommes d'argent à la vue de tous; si possible n'arborez pas de bijoux trop voyants.

Ne composez jamais votre code de carte bleue au vu et au su de tous; évitez absolument de marquer votre

code de carte de paiement sur un pense-bête mis dans votre portefeuille. Détruisez vos tickets de caisse payés avec carte bleue (car le n° de carte peut y figurer).

Si vous estimez être une personne vulnérable, faites vos plus grosses emplettes ou aller percevoir votre pension à deux ou en groupe.

Si vous croyez être suivi, traversez la rue, rapprochez-vous de passants, ou allez à la station-service ou dans le commerce le plus près et appelez le 17.

En général, signalez tout renseignement utile à la gendarmerie; celle-ci est toujours intéressée d'être informée et peut par ailleurs vous suggérer des moyens de vous protéger.

En cas d'agression pour vol, si votre intégrité physique n'est pas menacée, évitez de vous battre : vos valeurs ne valent pas d'être blessé ; si vous le pouvez, appelez au secours en criant fort ; notez le signalement précis de votre agresseur (âge apparent, taille, corpulence, couleur de peau, couleur des yeux, couleur et coupe de cheveux, signes particuliers, tics, accent, signes particuliers, tatouages ou bijoux, gaucher ou droitier...). Relevez les caractéristiques du véhicule qu'il utilise (couleur, marque, type, n° d'immatriculation même partiel, signe particulier, direction de fuite...).

En cas de vol de votre portefeuille, portez plainte en indiquant précisément le contenu de ce qui vous a été volé et faites rapidement les opérations nécessaires auprès de votre banque (opposition à carte bleue), de tout autre organisme ou assurance ou grande surface (opposition à carte de paiement), de votre opérateur téléphonique (suspension de ligne de téléphone portable), des administrations concernées (carte vitale, passeport, carte d'identité, permis de conduire...). Ceci évitera que ces moyens/documents soient utilisés à votre insu.

II -Les automobilistes: Il existe quelques règles élémentaires à suivre dans certaines situations. Sachez faire preuve de jugement afin de décider des mesures à prendre.

Verrouillez toujours les portières de votre véhicule en stationnement, ou même en marche. Au stationnement pensez aussi à mettre le frein à main, la sécurité de volant voire de votre équipement autoradio ou l'alarme si elles existent; pensez à ne laisser apparent aucun objet ou vêtement de valeur. Jamais ne laissez, même un seul instant, les clés sur votre véhicule.

La nuit, utilisez soit des garages privés, soit des stationnements publics éclairés.

Méfiez-vous des personnes inconnues qui s'approchent brusquement de votre véhicule. Si vous croyez être en danger, donnez plusieurs coups le klaxon; vous attirerez ainsi l'attention.

Si vous vous sentez suivi, arrêtez-vous à la station-service la plus près ou dans un endroit sûr et appelez la gendarmerie. Ne vous rendez pas jusque chez vous ou dans un endroit isolé.

Évitez de prendre des auto-stoppeurs, sauf si vous les connaissez.

Dans un endroit jugé peu sûr, ayez vos clés en main ou à portée immédiate de façon à pouvoir monter dans la voiture sans tarder. Une fois monté, verrouillez vos portières.

Signalez aussi à la gendarmerie tout vol de plaque d'immatriculation. Le voleur peut l'utiliser et se faire ainsi passer pour vous lors d'un de ses méfaits.

III - Les vols de téléphones portables: Il existe des actes réflexes pour s'en protéger.

En public, notamment dans une foule, pour éviter d'attirer les convoitises, soyez discret et vigilant lorsque vous utilisez un téléphone portable. Tenez-le fermement.

Ne prêtez pas votre téléphone mobile à un inconnu. Si quelqu'un vous demande d'appeler les secours, faites le vous-même en cas de doute.

Lorsque vous n'utilisez pas votre téléphone portable, ne le laissez pas à portée de vue mais rangez-le dans une poche. Ne le laissez pas traîner sur une table, sur un siège de voiture...

Personnalisez votre code PIN qui est demandé chaque fois que vous allumez votre portable.

En cas de vol, portez plainte. Pour ce faire, n'oubliez pas de communiquer le numéro d'identification de votre portable (n° IMEI à 15 chiffres) qui permettra à la gendarmerie d'inscrire votre téléphone au fichier des objets volés (pour le retrouver plus facilement).

Il est donc vivement conseillé de noter et de conserver chez soi le numéro IMEI, véritable plaque d'immatriculation de votre téléphone portable. Pour connaître à tout moment votre numéro IMEI, il suffit de composer sur le clavier de votre téléphone portable : * # 0 6 # .

En cas de vol, appelez bien sûr immédiatement votre opérateur pour suspendre votre ligne.

LA SÉCURITÉ SUR INTERNET

INFORMATION DESTINÉE AUX PARENTS :

- Sachez que certaines personnes s'inventent une identité sur internet. Des adultes peuvent prétendre avoir le même âge que votre enfant, juste pour apprendre à le connaître. Ils persévèrent parfois longtemps afin de gagner progressivement sa confiance.
- Surveillez l'usage que fait votre enfant d'internet. Participez à ses activités et posez-lui des questions sur ce qu'il fait et la manière dont il le fait.
- Réglementez l'utilisation d'internet. Fixez des limites quant au moment, à la durée et au type d'utilisation permis en fonction de l'âge et du degré de maturité de votre enfant (par ex. naviguer sur le net plutôt que de participer à des forums de discussion). Apprenez impérativement à votre enfant à ne pas divulguer de renseignements personnels à ses interlocuteurs virtuels.
- Installez l'ordinateur dans un endroit bien en vue et très passant de la maison afin de pouvoir régulièrement surveiller ce que votre jeune enfant fait sur internet. Évitez de le mettre dans sa chambre, même si cela semble pratique.
- Si vous vous inquiétez des sites que votre enfant consulte ou des forums de discussion auxquels il participe, parlez-en avec lui et communiquez avec votre fournisseur d'accès afin de connaître les logiciels disponibles pour bloquer l'accès à certains sites.
- Voici de simples conseils que vous pourrez partager avec vos enfants afin de leur permettre de naviguer sur internet en toute sécurité :

1) Assure-toi qu'un adulte est à proximité

Assure-toi que tes parents, un professeur ou un adulte digne de confiance est à proximité afin de pouvoir lui poser des questions ou demander de l'aide en cas de besoin.

2) Utilise un surnom

NE DIS JAMAIS ton nom à un inconnu avec qui tu communique sur internet. Invente-toi un surnom : fais preuve d'imagination!

3) Ne communique jamais de renseignements personnels

Ne donne jamais de renseignements personnels sans la permission d'un de tes parents. Ne dis à personne ton âge, ton adresse, ton numéro de téléphone fixe ou portable ou l'école que tu fréquentes. Tes mots de passe pour des sites "web" et ton courriel doivent également rester secrets. Ne donne jamais tes mots de passe.

4) N'envoie jamais de photos ou films

N'envoie jamais de photos ou films numériques de toi-même à un inconnu sur internet. Avertis tes parents ou un professeur si un inconnu veut t'envoyer une photo ou un film.

5) Vérifie auprès d'un adulte avant de télécharger quelque chose

Les fichiers et les programmes que tu télécharges peuvent contenir des virus, des contenus illicites, ou d'autres choses qui pourraient endommager ton ordinateur. Utilise un anti-virus.

6) Sois toujours courtois(e)

Évite d'être cruel envers tes "cyberamis". N'utilise jamais de mots impolis ou méchants. Ne diffuse pas de rumeurs ou de mensonges sur les gens. Si quelqu'un t'envoie des messages méchants, dis-le à tes parents ou à un professeur. Il vaut mieux éviter les chaînes de lettres et quitter toute conversation où les gens sont impolis.

7) Refuse d'acheter ou d'accepter des cadeaux

N'accepte jamais d'acheter un jouet, un jeu, un livre ou quoi que ce soit sans l'autorisation et la présence de tes parents. Refuse de participer à un concours ou de te joindre à un club sans permission. Ne permets jamais à quelqu'un de t'envoyer un cadeau gratuit.

8) N'accepte jamais de rencontrer ou d'appeler quelqu'un

Si un inconnu te demande de le rencontrer en personne, dis NON et avertis tout de suite tes parents ou un professeur. La personne avec qui tu communique ne dit peut-être pas la vérité; tu pourrais converser avec un adulte qui se fait passer pour un enfant.

9) Avertis tout de suite un adulte

Si tu vois quelque chose à l'ordinateur - un message ou une image - qui te met mal à l'aise ou te déplaît, dis-le à tes parents ou à un professeur sans tarder.

10) Si tu n'es pas sûr(e), demande conseil à quelqu'un

Tu ne sais jamais ce que tu vas trouver sur internet. Si tu n'es pas sûr(e) de la façon d'aborder une situation, demande conseil à un adulte.

INFORMATION DESTINÉE AUX ADOLESCENTS :

- Sachez que certaines personnes s'inventent une identité sur internet. Des adultes peuvent prétendre avoir le même âge que vous juste pour apprendre à vous connaître. Ils persévèrent parfois longtemps afin de gagner progressivement votre confiance.

- Ne divulguez aucun renseignement personnel vous concernant (comme votre adresse, votre numéro de téléphone, l'école que vous fréquentez, votre photographie, voire vos coordonnées bancaires) à vos interlocuteurs virtuels sans y avoir été autorisé par vos parents ou votre tuteur.

Agissez comme vous le feriez avec un étranger rencontré dans un parc.

- N'acceptez jamais de rencontrer un de vos interlocuteurs virtuels sans l'autorisation de vos parents ou de votre tuteur. Faites en sorte que vos parents ou votre tuteur assistent à vos premières rencontres. La première rencontre devrait toujours avoir lieu dans un lieu public.

- Ne répondez pas aux messages où l'on vous demande des renseignements personnels, à ceux qui sont mesquins ou qui vous mettent mal à l'aise. Vous n'êtes pas obligé de continuer; mettez fin à la communication et choisissez quelqu'un d'autre.

-Si vos parents sont d'accord pour un achat en ligne, vérifiez que le site est officiel et sécurisé pour ce type d'action: la mention "https" doit notamment figurer en début d'adresse électronique du site et le dessin d'un cadenas et/ou d'une clé doivent apparaître sur la page de paiement en ligne.

-N'oubliez pas que le piratage de films ou musiques sur internet est interdit et puni par la loi.

Pour signaler un fait particulier (images dégradantes, appels à la violence...) ou pour obtenir l'aide immédiate de la sécurité publique, communiquez avec la brigade locale de gendarmerie.

LA SÉCURITÉ INFORMATIQUE DANS L'ENTREPRISE

Même sans être sensibles, certaines petites et moyennes entreprises, mais aussi des collectivités territoriales ou administrations publiques déconcentrées, peuvent faire l'objet d'erreurs humaines ou d'actes malveillants à caractère informatique qui occasionneront parfois des préjudices socioéconomiques certains. Selon des études officielles, 50% des atteintes informatiques au sein de ces organismes ont des origines internes (volontaires ou involontaires).

Il existe pourtant des moyens simples de s'en protéger efficacement :

- Identifier clairement un « cœur » de l'information à protéger absolument au sein de l'entreprise/organisme. N'oubliez pas de faire des sauvegardes qui seront scrupuleusement protégées.
- Édicter une charte, à destination des employés et stagiaires, indiquant les mesures de précaution élémentaires à prendre en matière de sécurité informatique et des réseaux. Désigner si possible un responsable chargé du contrôle de l'application des dites mesures et du respect de la charte.
- Les ordinateurs aux informations sensibles doivent impérativement comporter un mot de passe (si possible 7 caractères alternant lettres, lettres avec accents, chiffres et caractères spéciaux), ce mot étant changé de préférence tous les 45 à 60 jours. Ces ordinateurs doivent être éteints ou mis en veille « disque dur » dès lors que le bureau n'est pas occupé pendant une période de plusieurs minutes, ceci afin de réactiver le processus de demande de mot de passe. Les ordinateurs contenant les informations les plus sensibles, non en réseau, doivent se situer dans des bureaux scrupuleusement fermés à clé. ■ Vos ordinateurs doivent être équipés d'anti-virus fiables avec mise à jour automatique. Vos employés doivent être sensibilisés au fait que tout document importé d'internet vers un ordinateur de l'entreprise par un support amovible (disquette, clé U.S.B...) doit être systématiquement passé à l'antivirus.
- Vos employés doivent être sensibilisés au fait que tout courriel de provenance inconnue, notamment lorsqu'il comporte des pièces-jointes, ne doit pas être ouvert mais effacé. Ce type de courriel est en effet le support idéal permettant l'entrée des virus dans votre ordinateur. De même, il est préférable d'éviter d'envoyer des informations confidentielles sur le réseau internet non crypté.
- Les employés, notamment cadres, doivent être sensibilisés aux risques de vols d'ordinateurs portables ou clés U.S.B., notamment lors de déplacements en dehors de l'entreprise (transports, hôtel, salon...) en France et à l'étranger. Pour ce faire, il est conseillé de ne conserver sur son ordinateur portable que les informations directement utiles à la mission concernée, afin de limiter les pertes de données sensibles en cas de vol. Il existe aussi des ordinateurs portables avec disque dur amovible.
- Il faut aussi savoir se méfier de certaines clés U.S.B. qui, branchées par un tiers sur votre ordinateur pour en apparence récupérer un seul document, permettent en fait, grâce à des programmes simples, de copier à votre insu tous les documents présents sur votre ordinateur.
- N'oubliez pas que certains photocopieurs évolués ont des disques durs qui ont enregistré toutes les photocopies effectuées. Spécifiez donc dans le contrat d'entretien de ces photocopieurs que leurs disques durs ne quittent pas l'entreprise s'ils sont susceptibles d'avoir photocopié des informations sensibles. Ne laissez pas traîner des photocopies ou notes sensibles; conservez-les ou détruisez-les. Par ailleurs, les photocopieurs identifiés comme « sensibles » peuvent être équipés d'un mot de passe.
- Précisez le champ d'informations auquel vos stagiaires ont accès; vérifiez le contenu de leurs rapports de stage. Soyez vigilants avec les intervenants extérieurs chargés de la réparation informatique.

LA SÉCURITÉ DES COMMERÇANTS

Les commerçants sont trop souvent les victimes des malfaiteurs mais des comportements simples peuvent prévenir certaines agressions.

Protégez votre commerce contre le vol à l'étalage

- Sécurisez vos articles de valeur.
- Soyez vigilant avec les groupes de personnes qui essaient de détourner votre attention.
- Ayez une bonne visibilité des locaux de votre commerce en supprimant si possible les angles morts ou en installant des dispositifs de vision adéquats (caméras, glaces..).

Protégez-vous contre les escroqueries aux moyens de paiement

- Vous pouvez demander la présentation d'une pièce d'identité pour tout paiement par chèque. S'il s'agit d'un chèque de société, exigez aussi un extrait K-Bis.
- Renseignez-vous auprès de votre banque sur les systèmes de vérification des chèques en opposition.
- En cas de doute sur la qualité d'un billet ou d'une pièce, refusez le (la).

Protégez votre commerce contre le cambriolage

- Faites blinder ou du moins renforcer tous les ouvrants sans négliger les portes arrières ainsi que les fenêtres ou vélux (beaucoup d'effractions ont lieu par les hauts ou l'arrière).
- Faites poser une grille ou un volet de protection devant votre devanture.
- Vous pouvez aussi faire installer :

- une lampe intensive qui s'allume grâce à un capteur lorsqu'une personne inconnue s'approche d'une zone privative sensible (arrière-cour du commerce p.ex.): les voleurs n'aiment pas la lumière,

-un film anti-effraction ou une vitre blindée sur votre vitrine,

-une alarme éventuellement couplée avec un système de dispersion de fumées aveuglantes,

-une ou des caméras de vidéo surveillance couplées à un magnétoscope non accessible.

- Au besoin, engagez une société de gardiennage qui pourra être automatiquement avertie par l'alarme.

- Ne remettez les clefs, codes... qu'à vos plus proches collaborateurs.

- Si votre commerce est sensible, protégez-vous contre les véhicules-béliers :

-en zone isolée, installez des obstacles (plots de béton, bacs de fleurs...),

-en zone urbaine, cette mesure requière l'autorisation de votre mairie.

- En règle générale, inventoriez tous vos matériels ou objets de valeur en relevant les marques et les numéros de série. Cela facilitera les recherches et l'identification en cas de découverte chez un receleur.

Protégez votre recette

- Soyez particulièrement vigilant lors de l'ouverture et de la fermeture de votre commerce.

- Ne conservez pas longtemps de fortes sommes dans votre caisse. Placez-les dans un endroit sûr: de préférence une banque, à défaut un coffre.

- Le coffre, s'il existe, doit être placé dans un endroit discret, non à la vue du public, le code connu d'un nombre minimum de personnes; ce coffre, ou la pièce le contenant, doit être si possible sous alarme; et surtout, le coffre doit être scellé au mur ou au sol; car un coffre non scellé ne sert presque à rien !

- Soyez particulièrement vigilant lorsque vous transportez des fonds à la banque. Évitez les déplacements à heure fixe et variez vos itinéraires. Si vous vous sentez suivi, évitez de vous retrouver isolé ou rentrez dans un endroit fréquenté, et appelez la gendarmerie. Protégez votre véhicule

- Le jour, ne laissez pas votre véhicule de société stationné sans surveillance ou sans alarme, dès lors qu'ils contiennent du matériel ou de la marchandise. Verrouillez coffre, portes ; bloquez le volant et le frein à main.

- Même pour une simple livraison, ne laissez pas dans votre véhicule vos papiers, chèquiers, doubles de clefs ou autres objets de valeur.

- Ne vous absentez pas de votre véhicule moteur en route avec les clefs sur le contact.

- La nuit, évitez de laisser votre véhicule à l'extérieur. Si vous y êtes obligé, stationnez toujours en zone éclairée, de préférence sous alarme.

- Si vous dormez dans votre véhicule de transport de marchandises la nuit, recherchez les parkings collectifs éclairés afin de n'être pas seul, et enfermez-vous dans votre véhicule.

- Un tag appelle d'autres tags. Ne laissez donc pas se multiplier les tags sur votre bâtiment. Prévenez les services techniques de votre mairie ou une société privée spécialisée pour les nettoyer.

- Signalez à la gendarmerie, en étant précis, toute personne à l'attitude suspecte dans ou aux abords de votre commerce qui serait susceptible de faire du "repérage".

- Portez plainte à la gendarmerie si vous êtes victime d'un méfait, quel qu'il soit. Essayez d'être précis sur le signalement du ou des agresseurs/malfaiteurs (âge apparent, taille, corpulence, couleur de peau, couleur des yeux, couleur et coupe de cheveux, signes particuliers, tics, accent, signes particuliers, tatouages ou bijoux, gaucher ou droitier...) et du véhicule utilisé (couleur, marque, type, n° d'immatriculation même partiel, signe particulier, direction de fuite...).