REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE LA POSTE ET DES TELECOMMUNICATIONS

Guide sur le commerce électronique

Janvier 2024

Guide sur le commerce électronique

Sommaire

L'adoption massive, par les citoyens, des transactions commerciales réalisées par voie de communications électroniques a suscité la réaction des autorités publiques afin de mettre en place une règlementation visant à instaurer un environnement de commerce électronique sûr et à protéger les consommateurs à travers la promulgation de la loi n05-18° du 10 mai 2018 qui fixe les règles générales relatives au commerce électronique.

Cependant, avec la croissance rapide du e-commerce est venue une augmentation parallèle des escroqueries en ligne en dépit du cadre juridique mis en place. Des escroqueries de tout genre ayant plusieurs sources de fraude liées aux appareils et aux logiciels utilisés pour les achats et d'autres sont liées aux modes de paiement ou bien du processus d'achat en général.

Afin de prévenir les escroqueries en ligne et garantir la confiance des utilisateurs, le Ministère des Postes et des Télécommunications, en collaboration avec l'ensemble des parties prenantes, a préparé ce guide, qui s'inscrit dans le cadre de la mise en œuvre des instructions émises par les hautes autorités du pays visant à concrétiser la feuille de route proposée par l'Autorité nationale pour la prévention des infractions liées aux technologies de l'information et de la communication afin de réduire les risques d'escroquerie en ligne.

Ce Guide se veut être un recueil présentant le cadre conceptuel, les risques liés au commerce électronique et met en évidence les dispositions sur le commerce électronique prévues dans la loi n05-18°, sus-citée, ainsi que les orientations à respecter pour les achats en ligne sécurisés.

Il prévoit aussi des conseils et des mesures à adopter en cas de fraude et escroquerie.

Il convient de noter que ce guide a été préparé conjointement par les secteurs, institutions et organes suivants:

- Ministère des Postes et des Télécommunications,
- Ministère du Commerce et de la Promotion des Exportations,
- Ministère des Finances,
- Gendarmerie Nationale
- Direction Générale de la Sureté Nationale,
- Algérie Poste,
- Groupement d'Intérêt Economique Monétique (G.I.E Monétique.)

I. Cadre conceptuel et risques liés au commerce électronique

1. Concepts de base :

Au regard de la croissance rapide des transactions commerciales en ligne ces dernières années et suite à l'augmentation remarquable de la demande des citoyens et des entreprises en matière de vente et d'achat en ligne. Les pouvoirs publics ont élaboré un cadre juridique pour ce type de transactions à travers la promulgation de la loi n° 05-18 du 10 mai 2018 fixant les règles générales du commerce électronique dont les concepts de base de ce texte, sont exposés ci-dessous, pour faciliter la compréhension du cadre général, des parties prenantes et des aspects juridiques et réglementaires du commerce électronique.

- Commerce électronique :

L'article 6 de la loi n05-18° définit le commerce électronique comme "activité par laquelle un e-fournisseur propose ou assure, à un e-consommateur, à distance et par voie de communications électroniques la fourniture de biens et de services".

- E-fournisseur:

toute personne physique ou morale qui commercialise ou propose la fourniture des biens ou des services par voie de communications électroniques.

- E-consommateur:

toute personne physique ou morale qui acquiert, à titre onéreux ou gratuit, un bien ou un service par voie de communications électroniques auprès d'un e-fournisseur pour une utilisation finale.

- Communications électroniques :

Communications électroniques : toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images ou de sons, de données, ou de renseignements de toute nature par fil, voie optique ou électromagnétique. (Art.10. Loi n04-18° fixant les règles générales relatives à la poste et aux communications électroniques).

- Contrat électronique :

contrat au sens de la loi n° 02-04 du 23 juin 2004 fixant les règles applicables aux pratiques commerciales, conclu à distance sans la présence physique simultanée des parties par le recours exclusif à une technique de communication électronique.

- Moyen de paiement électronique :

tout instrument de paiement, autorisé conformément à la législation en vigueur, permettant à son titulaire d'effectuer des paiements de proximité ou à distance à travers un système électronique.

- Publicité électronique :

toute annonce ayant pour objectif direct ou indirect de promouvoir la vente de biens ou de services par voie de communications électroniques.

- Précommande :

engagement de vente qui peut être proposé par le e-fournisseur au e-consommateur en cas d'indisponibilité du produit en stock.

- Nom du domaine :

chaîne alphanumérique normalisée enregistrée au niveau du registre national des noms de domaine et qui permet d'identifier le site électronique et d'y accéder.

2. Principaux risques liés au commerce électronique:

Les acheteurs en ligne sont confrontés à un certain nombre de risques qui peuvent les conduire à être victimes d'escroquerie et de fraude. Certains risques sont liés aux appareils et programmes utilisés lors des achats en ligne, d'autres sont liés aux moyens de paiement, tandis que le reste se rapporte aux modalités et processus d'achat, en général.

Les principaux risques peuvent être résumés comme suit :

- La propagation de nombreux sites web, de pages et de plateformes qui proposent aux consommateurs des biens et des services très demandés à bas prix avec des remises très attractives, dans le but de l'arnaquer.
- Le vol d'identité ou des cartes de crédit des acheteurs en ligne, et l'utilisation de leurs données personnelles dans des opérations d'achat en ligne, mettant les coûts des biens et services à leur charge,
- L'importation des marchandises prohibées à la commercialisation sur les marchés locaux,
- Risque de piratage des cartes de paiement et des données personnelles notamment à travers les courriels de sources inconnues, les faux sites web, les applications électroniques et les logiciels douteux.
- Risque lié à la réalisation de transactions avec des fournisseurs non identifiés en raison de la nature et la spécificité de la transaction commerciale dans la sphère virtuelle, ce qui rend difficile l'obtention des preuves matérielles en cas de dépôt de plainte.

II. Conseils relatifs aux transactions commerciales électroniques conformément aux dispositions de la loi n05-18°

Cet axe comprend des conseils relatifs aux transactions commerciales électroniques conformément aux dispositions de la loi n° 18-05 relative au commerce électronique. A ce titre, nous aborderons le champ d'application du commerce électronique, ses conditions et exigences, ainsi que les droits et obligations de ses parties.

1. champs d'application de la loi

La loi algérienne est applicable en matière de transactions commerciales électroniques dans le cas où l'une des parties du contrat électronique est:
- De nationalité algérienne, ou
- Réside légalement en Algérie, ou
- Une personne morale de droit algérien,
- Ou si le contrat est conclu ou exécuté en Algérie.

Toutefois, est interdite toute transaction par voie de communications électroniques portant sur:
- Les jeux de hasard, paris et loteries,
- Les boissons alcoolisées et tabac,
- Les produits pharmaceutiques,
- Les produits portant atteinte aux droits de propriété intellectuelle, industrielle ou commerciale,
- Tout bien ou service prohibé par la législation en vigueur,
- Tout bien ou service qui requiert un acte authentique,
- Matériels, équipements et produits sensibles définis par la réglementation en vigueur,
- tout autre produit et/ou services pouvant porter atteinte aux intérêts de la défense nationale, à l'ordre et à la sécurité publics.

2. Conditions et exigences de l'e-fournisseur

a) Conditions d'exercice du commerce électronique:

Pour l'exercice du commerce électronique dans le cadre de la législation et de la réglementation en vigueur, il est impératif de respecter les conditions prévues dans l'article 8 de la loi n°18-05, à savoir :
- Inscription au registre du commerce ou au registre de l'artisanat et des métiers,
- Publication d'un site, ou page web hébergé en Algérie,
- Obtention du nom du domaine avec une extension "com.dz ",
- Le site web doit être muni des outils permettant son authentification,
- Dépôt du nom de domaine auprès des services du Centre National du Registre du Commerce.

- Conditions de la transaction commerciale :

Toute transaction commerciale doit se conformer aux conditions suivantes :
- Toute transaction de commerce électronique doit être précédée par une offre commerciale électronique,
- Formaliser la transaction par un contrat électronique,
- Le e-consommateur doit valider le contrat électronique.

Note : en cas de non-respect desdites conditions par le e-fournisseur, le e-consommateur peut demander l'annulation du contrat et de recevoir des dommages et intérêts.

b) Exigences de l'offre commerciale électronique :

L'offre commerciale électronique doit être présentée de manière visible, lisible et compréhensible. Elle doit comporter, sans toutefois s'y limiter, les informations suivantes :
- Le numéro d'identification fiscale, les adresses physique et électronique ainsi que le numéro de téléphone du e-fournisseur ;
- Le numéro de registre du commerce ou le numéro de la carte professionnelle d'artisan ;
- La nature, les caractéristiques et le prix des biens ou services proposés en toutes taxes comprises.
- L'état de disponibilité du bien ou du service,
- Les modalités, les frais et les délais de livraison,
- Les conditions générales de vente, notamment les indications relatives à la protection des données à caractère personnel,
- Les conditions de garantie commerciale et du service après-vente,
- Le mode de calcul du prix, lorsque celui-ci ne peut être fixé à l'avance,
- Les modalités et les procédures de paiement,
- Une description complète des différentes étapes d'exécution de la transaction électronique,
- La durée de l'offre, le cas échéant,
- Les conditions et les délais de rétractation, le cas échéant,
- Le mode de confirmation de la commande,
- Le délai de livraison, le prix du produit objet de la précommande et les modalités d'annulation de la précommande, le cas échéant,
- Le mode de retour du produit, d'échange ou de remboursement,
- Le coût d'utilisation des moyens de communications électroniques lorsqu'il est calculé sur une autre base que les tarifs en vigueur.

c) Contenu du contrat électronique :

Le contrat doit comporter les informations suivantes :
- Les spécifications détaillées des biens ou des services,
- Les conditions et modalités de livraison,
- Les conditions de garantie et de service après-vente,
- Les conditions de résiliation du contrat électronique
- Les conditions et modalités de paiement ;
- Les conditions et modalités de retour du produit,
- Les modalités de traitement des réclamations,
- Les conditions et modalités de précommande, le cas échéant,
- Les conditions et modalités particulières liées à la vente à essai, le cas échéant,
- La juridiction compétente, en cas de litige,
- La durée du contrat selon le cas,

Note : Dans le cas du non-respect de ces dispositions l'e-consommateur peut demander l'annulation du contrat et de recevoir des dommages et intérêts.

d) Obligations et responsabilités du e-fournisseur:

La conclusion du contrat implique les responsabilités et les obligations du e-fournisseur et ce comme suit :
- Après conclusion du contrat électronique, le e-fournisseur est responsable de plein droit de la bonne exécution des obligations résultant de ce contrat, que ces obligations soient à exécuter par lui-même ou par d'autres prestataires de services,
- Transmission d'une copie électronique dudit contrat à l'e-consommateur.
- Etablissement d'une facture conformément à la législation et à la réglementation en vigueur et la remettre au e-consommateur,
- Reprise du produit en l'état en cas de non-respect des délais de livraison,
- Reprise de la marchandise, en cas de livraison d'un article non conforme à la commande ou dans la cas d'un produit défectueux,
- Le e-fournisseur ne doit pas valider la commande d'un produit non disponible en stock,
- Conservation des registres des transactions commerciales réalisées ainsi que leurs dates et les transmettre, par voie électronique, au Centre National du Registre du Commerce,
- Le e-fournisseur ne doit recueillir que les données à caractère personnel nécessaires à la conclusion des transactions commerciales, après l'accord préalable de l'e-consommateur tout en garantissant la sécurité des systèmes d'information et la confidentialité des données.

3. Droits et obligations du e-consommateur:

3. 1. Droits du e-consommateur :

- Recevoir une copie électronique du contrat après sa conclusion,
- Recevoir la facture de l'e-fournisseur,
- Recevoir un produit conforme à la commande, non défectueux et dans le délai de livraison,
- Possibilité de réexpédier le produit en l'état non conforme à la commande ou défectueux ou dans le cas de non-respect des délais de livraison,

3. 2. Obligations de l'e-consommateur

- Paiement du prix convenu dans le contrat électronique dès sa conclusion, sauf stipulations contraires prévues dans le contrat électronique,
- Signature de l'accusé de réception dès la livraison effective du produit ou à la fourniture du service objet du contrat électronique,
- Récupération d'une copie de l'accusé de réception.

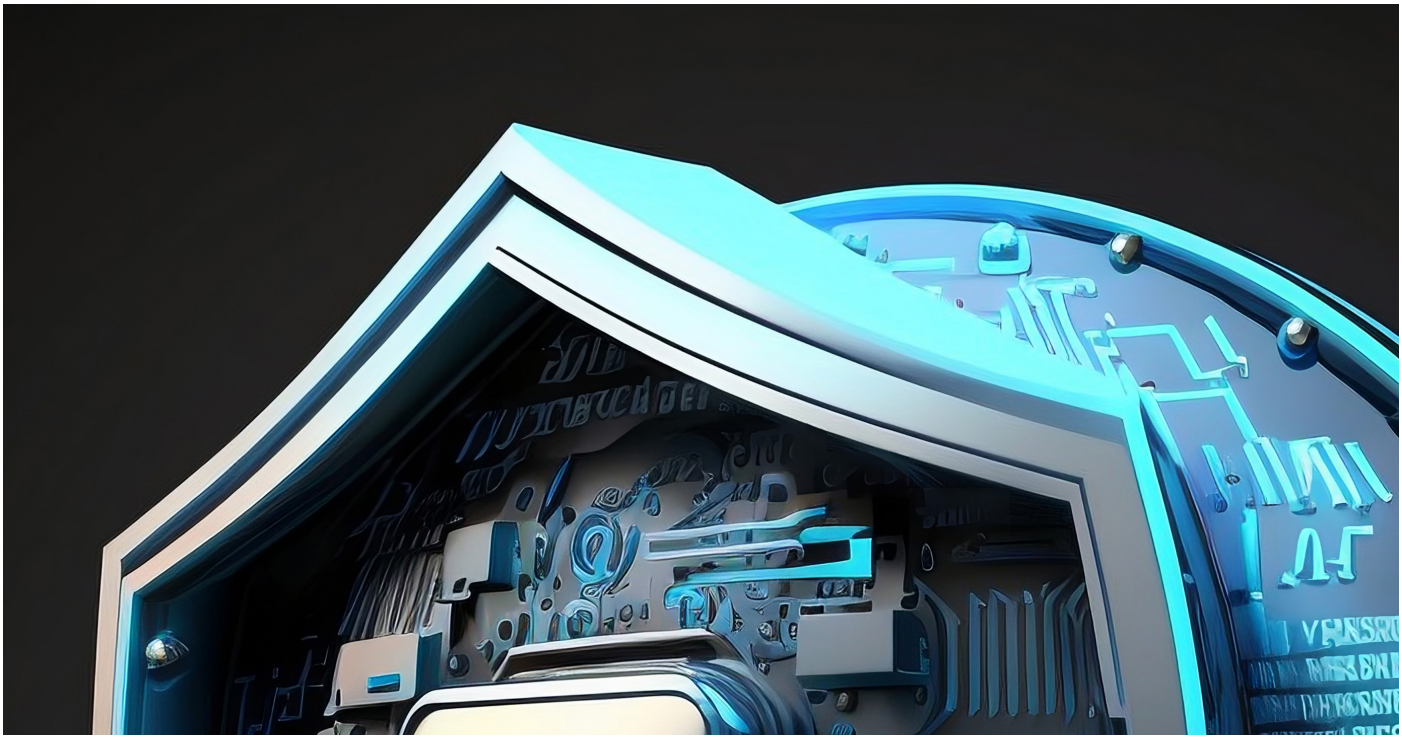
4. Paiement des transactions commerciales électroniques

Le paiement des transactions commerciales électroniques s'effectue, à distance ou à la livraison du produit, par les moyens de paiement autorisés conformément à la législation en vigueur.

Lorsque le paiement est électronique, il s'effectue à travers des plates-formes de paiement dédiées, mises en place et exploitées exclusivement par les banques agréées par la Banque d'Algérie et Algérie Poste et connectées à tout type de terminal de paiement électronique via le réseau de l'opérateur public de télécommunications.

Le paiement des transactions commerciales transfrontalières s'effectue exclusivement à distance par voie de communications électroniques.

La connexion du site web de l'e-fournisseur à une plate-forme de paiement électronique doit être sécurisée par un système de certification électronique.



III. Conseils pour un acte d’achat en ligne sécurisé

Cet axe inclut des conseils de sensibilisation destinée aux fournisseurs et aux consommateurs impliqués dans tout processus d'achat en ligne, contribuant à garantir une expérience d'achat en ligne sécurisé.

- Conseils d'ordre général :

1- Utilisation de logiciels antivirus fiables

L'installation sur les appareils, particulièrement ceux fréquemment utilisés dans le e-commerce (PC, téléphones et tablettes smart), de logiciels antivirus fiables téléchargés à partir des sites officiels ou acquis auprès de fournisseurs agréés, ainsi que leur mise à jour constante, concourent à assurer, à l'utilisateur, une expérience d'achat sécurisée en ligne, que ce soit lors de communications, d'échanges de messages ou d'opérations commerciales sur Internet.

2. Utilisation des applications sécurisées

Il est recommandé de télécharger des applications pour les téléphones et les tablettes smart, exclusivement à partir de sources officielles et fiables, via des supports agréés, à l'instar de (App Store) pour iOS ou (Google Play) pour Android ou (Huawie AppGallery) pour HarmonyOS. Il est, également recommandé de consulter les avis d'autres utilisateurs sur les supports de téléchargement des applications.
Les applications installées sur les appareils doivent également être mises à jour automatiquement ou manuellement, via les supports de téléchargement.

3. Utilisation des mots de passe efficaces

Il convient d'utiliser des mots de passe fiables et complexes comprenant des lettres (majuscules et minuscules), des chiffres et symboles, tout en évitant les mots courants et fréquents ou ceux incluant des informations personnelles ou une simple séquence de chiffres ou de lettres, ainsi que l'utilisation du même mot de passe sur l'ensemble des sites web, comptes et applications, pour éviter le piratage et la divulgation des données personnelles.
Il est également recommandé de changer périodiquement les mots de passe et d'éviter de les partager.

4. Activation de la double authentification

Cette fonctionnalité constitue un mécanisme supplémentaire de protection des comptes, notamment en cas de piratage du mot de passe. Elle peut être activée pour empêcher quiconque d'accéder au compte, car le titulaire du compte peut se connecter à l'aide d'un mot de passe envoyé au téléphone portable.

5. Préservation des données personnelles :

Il est recommandé, à cet effet, d'accorder une grande importance à la préservation des données personnelles, et d'éviter de les partager, notamment celles inhérentes aux cartes de paiement et aux comptes personnels.

6. Modification des paramètres par défaut sur l'appareil de l'utilisateur

Il est nécessaire de vérifier et de modifier les paramètres par défaut du compte utilisateur et du navigateur Internet, pour éviter d'enregistrer les informations de connexion, les données de paiement électronique, les comptes postaux ou bancaires.

7. Etre prudent quant aux e-mails, communications et annonces publicitaires

A cet égard, il est conseillé d'être prudent quant aux:
- spams, procéder à l'activation du système de filtrage,
- messages trompeurs comme : «Dépêche-toi, quantité limitée «, « inscrit-toi pour gagner des prix» etc.,
- messages frauduleux : destinés aux tentatives de fraudes et escroqueries à l'encontre du consommateur,
- annonces d'avertissement: il est recommandé de lire et saisir rigoureusement et de traiter ces annonces avec précaution,
- Communications frauduleuses: des communications peuvent provenir de faux commerçants possédant de faux sites web.

8. Utilisation d'appareils et de sites web sécurisés

Il est recommandé, à cet effet, d'éviter l'utilisation des appareils publics et d'utiliser uniquement un appareil personnel lors des achats en ligne, afin de protéger les informations personnelles et les données des comptes financiers.
il est impératif, en sus, d'éviter l'enregistrement des informations personnelles et des données des cartes magnétiques ou bancaires sur un appareil connecté à un réseau Internet public.
Par ailleurs, et avant d'effectuer toute opération d'achat en ligne, il faut s'assurer que le lien du site

web commence par (https://) au lieu de (http://), car ces sites sont protégés par des protocoles de cryptage fiables.

9. Consultation des conditions d'utilisation du site web d'achats et de la politique de confidentialité

Dans ce contexte, il est recommandé de repasser en revue, notamment les éléments suivants:
- La politique de confidentialité, est un ensemble de règles et de conditions explicitant la manière dont les informations des visiteurs du site web sont collectées, utilisées et échangées.
- Le nom du vendeur et les produits affichés sur le site,
- Les appréciations et avis d'autres utilisateurs sur les produits, pour vérifier la qualité du produit,
- Les politiques de retour et d'échange du produit,
- La présence de l'accusé de paiement.

10. Vérification et examen de la nature du produit

Avant de choisir le produit, il est indispensable de s'assurer qu'il ne figure pas sur la liste des marchandises interdites à l'importation ou à la circulation. Dès réception, il faut bien examiner le produit et s'assurer qu'il est en bon état et non périmé, conformément aux conditions convenues avec le fournisseur.

- Conseils liés au processus de paiement

- Il est nécessaire de connaître le numéro d'urgence de la banque, de l'institution financière ou du centre d'appels.
- Placer les cartes de paiement dans des endroits sûrs.
- Éviter de sauvegarder le code secret de la carte sur l'ordinateur ou les comptes électroniques, ou de l'envoyer par e-mail.
- Eviter de conserver le code secret avec la carte pour éviter tout risque de fraude.
- Eviter de partager le code secret avec toute personne, y compris les responsables des clients, les conseillers financiers affiliés à l'entreprise «Algérie Poste» ou aux établissements bancaires.
- Examiner périodiquement les comptes financiers pour s'assurer de l'absence d'opérations suspectes, le cas échéant, contacter immédiatement l'établissement postal ou bancaire de l'utilisateur en cas de doute de transactions frauduleuses.
- Activer les notifications par SMS relatifs aux comptes courant postal ou bancaire, pour permettre à l'utilisateur de recevoir des alertes concernant toute transaction financière effectuée sur son compte.
- Activer, sur la ligne téléphonique mobile du détenteur de la carte monétique, la notification via SMS de tout processus de paiement en ligne. Changer le numéro de téléphone en cas de perte, cession ou modification, pour éviter toute éventuelle confirmation d'achat, via SMS, par une autre personne utilisant l'ancien numéro de téléphone.
- A l'étape de paiement, il faut s'assurer que la nouvelle fenêtre de paiement affiche l'une des adresses suivantes :

- https://epay.poste.dz ou https://cib.satim.dz sinon, évitez de saisir vos données.

- Les informations requises lors de l'opération de paiement par la carte monétique sont :

- Le numéro de carte qui est composé de 16 chiffres,
- La date d'expiration,
- Le code de sécurité et de protection qui figure au dos de la carte, composé de 3 chiffres,
- Le nom et prénom,
- Avant de confirmer l'opération de paiement, il faut s'assurer que le montant de la transaction indiqué ou affiché sur la page de paiement correspond à celui affiché sur le site marchand,
- Eviter de sauvegarder les informations de la carte magnétique sur le site marchand,
- En cas de perte de la carte monétique, il faut procéder au blocage immédiat de celle-ci, par tous les moyens disponibles (centres d'appels, bureaux de poste, agences bancaires, applications de caisse,...).

V. Orientations tirées d’expériences des cas de fraudes et d’escroqueries constatés

Les constatations sur le terrain, par les services de sécurité et les des différentes parties prenantes au domaine des transactions commerciales électroniques en Algérie, font ressortir l'observation de transactions commerciales en ligne considérées par les citoyens en tant que transactions de commerce électronique s'effectuant via les pages de réseaux sociaux et autres sites web ne répondant pas aux exigences et règles du commerce électronique tel que stipulé dans la loi 18-05.
L' on note, par ailleurs, la propagation et la multiplication de sites Web, de pages et de plateformes proposant au consommateur des biens et services extrêmement demandés, à bas prix, avec des remises très attractives, dans un but frauduleux, en sus de la propagation et la diversification des moyens de fraudes et d'escroqueries à l'occasion des opérations d'achat en ligne.
A cet égard, nous essayerons, d'aborder, ci-dessous, les techniques de fraude et d'escroquerie les plus fréquemment enregistrées, et ensuite de fournir des conseils et des orientations préventifs à recommander en cas de fraude et d'escroquerie.

1- Principaux moyens de fraudes et d'escroqueries enregistrés:

Les opérations frauduleuses les plus répandues dans la société algérienne sont celles ayant eues cour sur les pages de réseaux sociaux, lesquelles opérations sont généralement exécutées par des web marchands fictifs qui opèrent en dehors du cadre légal institué par les règles générales relatives au commerce électronique, ou affichant sur leurs pages web des produits, des biens et services très demandés et à moindre tarifs, proposant des remises très attractives, ayant pour but d'arnaquer le consommateur, à l'occasion desquelles le fraudeur reçoit des virements ou des avances via son compte postal ou bancaire ou en utilisant le service de transfert de fonds disponibles sur les applications mobiles des établissements financiers, sans effectuer l'envoi du produit au demandeur.
Les fraudeurs emploient plusieurs techniques et méthodes pour arnaquer et tromper les citoyens.

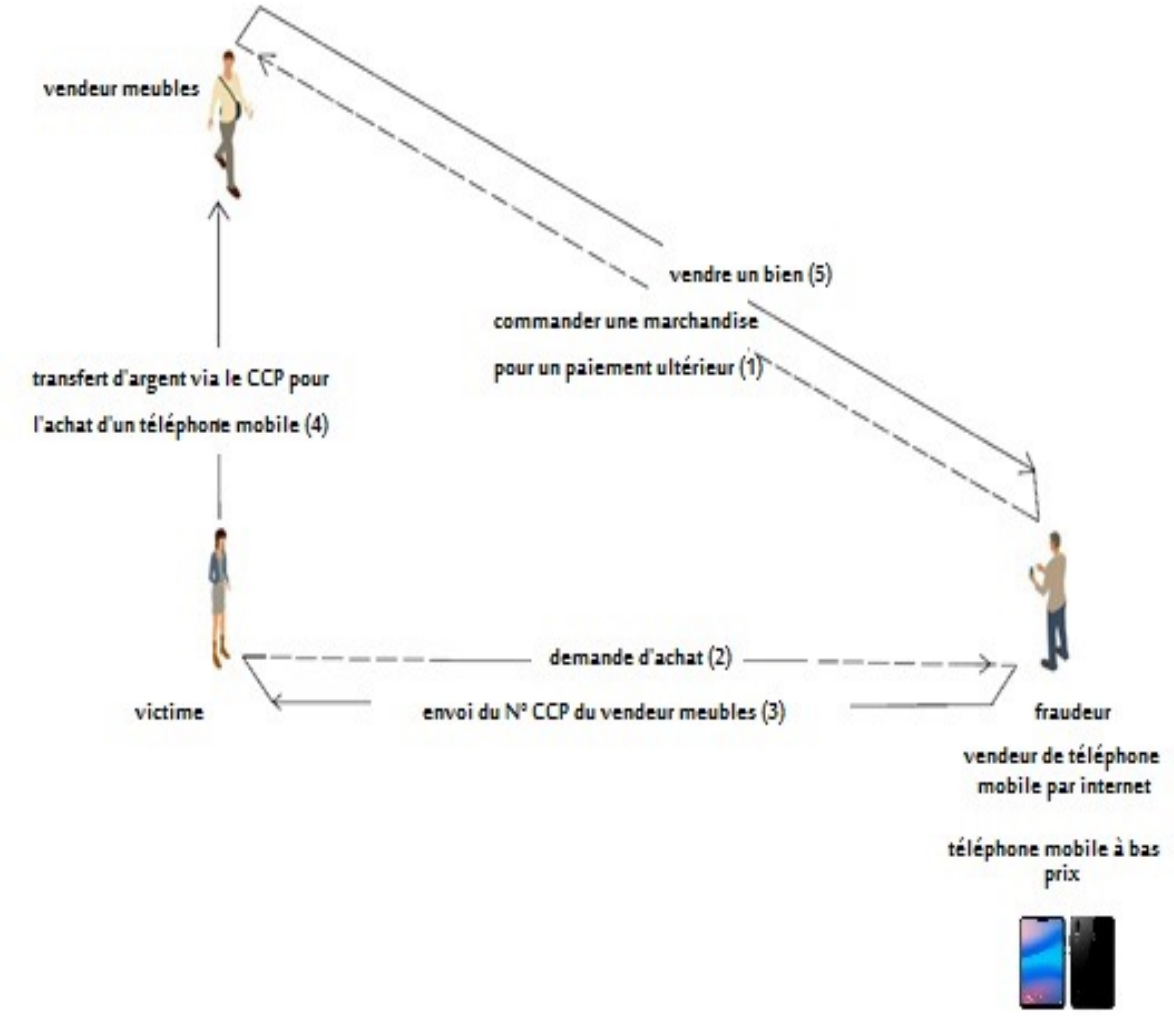
- l'imitation de sites web: utilisée le fraudeur pour persuader le consommateur qu'il traite avec des parties réputées et crédibles ou avec des e-fournisseurs légaux.

- l'urgence : le fraudeur emploie le caractère urgent pour tromper le consommateur à travers de mettre, en mettant en évidence l'importance de l'offre et la courte durée de l'offre, tout en signalant l'urgence de lui faire parvenir rapidement la commande pour éviter de rater l'opportunité. Il peut, ainsi, requérir le virement de fonds, de fournir des informations personnelles ou de cliquer sur des liens nuisibles.

- la manipulation émotionnelle: le fraudeur emploie cette méthode pour manipuler les sentiments des consommateurs et susciter leurs émotions, afin de les convaincre du bien fondé de ses intentions, et les persuader d'exécuter ce qu'il désire, comme envoyer du fonds ou acheter un produit.
- la fraude et l'escroquerie s'appuyant sur des messages frauduleux: cette opération consiste en l'usurpation de l'identité de l'entreprise «Algérie Poste», en utilisant, pour induire en erreur les potentielles victimes, l'envoi aux téléphones des victimes de messages frauduleux courts arborant l'appellation «ALG Poste», confirmant le paiement sur leur compte courant postal, pour prouver le paiement des achats ou confirmer les transactions commerciales effectuées à distance.
Les messages frauduleux parvenant aux appareils des victimes ont un contenu et une forme similaires à ceux adressés, effectivement, par l'entreprise «Algérie Poste» à ses clients ayant activés le service de suivi des comptes postaux par téléphone et ce, à travers l'utilisation par les fraudeurs de plateformes et sites web internationaux par des fraudeurs transmettant des SMS dans le monde entier, profitant de la possibilité de procéder à la falsification du nom de l'expéditeur et son remplacement par l'appellation «Algérie Poste», et ce afin de tromper leur victimes et leur faire croire que le message a été envoyé depuis la plateforme numérique d'Algérie Poste et que des sommes d'argent avaient été versées sur leurs comptes.

- la triple fraude: cette méthode s'appuie sur trois parties, le faux marchand (l'imposteur), le fournisseur réel (victime) et le consommateur (victime), et passe par les étapes suivantes :

- Le fraudeur achète d'abord une marchandise ou un service au fournisseur réel et accepte que le paiement soit effectué par l'intermédiaire d'un compte bancaire ou d'un compte postal ;
- à l'étape suivante, le fraudeur présente le bien ou le service via les sites des réseaux sociaux, et convient avec le consommateur d'envoyer le montant de la marchandise fictive via un compte courant postal ou un compte bancaire appartenant en réalité au fournisseur réel ;
- après avoir confirmé le paiement par l'acheteur du montant convenu, le fraudeur bloque ce dernier sur toutes les plateformes des réseaux sociaux, puis se retire et implique le fournisseur réel avec le consommateur (victime).



2/ Orientations préventives en cas de fraude et d'escroquerie

Dans le cas d'une escroquerie en ligne, il est recommandé de garder son calme. Il est normal de ressentir de la colère ou de ressentir de la frustration après avoir été victime d'une escroquerie, mais il est important de demeurer serein et de procéder à la mise en œuvre des actions suivantes:

- Recueillir un maximum d'informations sur l'escroquerie, notamment les délais de l'opération (compte fraudeur, montant, messages électroniques échangés, captures d'écran, liens ou page web,...),
- Se rendre immédiatement au poste de service de sécurité le plus proche (la police ou la gendarmerie nationale selon la compétence territoriale), pour signaler l'escroquerie, appuyés par les éléments d'informations recueillies sur l'opération.
- En cas de difficulté de signalement par déplacement aux sièges des services de sécurité, vous pouvez appeler les numéros verts gratuits disponibles : la police 1548, la Gendarmerie Nationale 1055, l'Organisation de Protection des Consommateurs 3311, le Ministère du Commerce et de la Promotion des Exportations. 1020, ou bien de procéder à un signalement à travers les deux liens des services de sécurité mis à la disposition des consommateurs.

- La Police algérienne : contactccp@algeriepolice.dz

- La Gendarmerie Nationale : https://www.mdn.dz/site_cgn/sommaire/services/ppgn/ppgn_ar.php

Il est également possible de :

- déposer une plainte auprès des services compétents du Ministère du Commerce et de la Promotion des Exportations.
- signaler à travers le site web ou les pages des réseaux sociaux des services de sécurité, chaque compte, page web ou publication frauduleuse, en vue de l'interdire et d'empêcher la survenance d'autres fraudes, à l'avenir.
- bloquer la carte magnétique, notamment en cas de vol de renseignements ou de suspicion d'une opération frauduleuse.