



People's Democratic Republic of Algeria
Ministry of Post and Telecommunications

GUIDE OF E-COMMERCE

January 2024

Guide of e-commerce

Guide plan

I-Conceptual framework and hazards related to e-commerce

1. Basic concepts
2. Main hazards related to e-commerce

II-Guidelines about e-commerce transactions pursuant to law 05-18

1. Application of the law
2. Terms and conditions of e-provider
3. Rights and obligations of e-consumer
4. Payment in e-transactions

III-Guidelines for a safe shopping online

1. General guidelines
2. Guidelines about payment transaction

IV. Guidelines stemming from registered swindling and fraud

1. Main ways and methods of registered swindling and fraud
2. Guidelines about the attitude to adopt in case of swindling or fraud



Following the widespread use and significant development of commercial transactions via e-communications in our country, public authorities have framed these transactions by enacting law 05-18 of May 10th, 2018 setting the general rules of e-commerce.

E-consumers can be faced to many risks likely to make them victims of swindling and fraud, although the aforementioned transactions are framed. This is due to the fact that some risks are associated to equipment and software used in shopping, some others concern the means of payment, while many other risks relate to the purchasing process in general.

To avoid fraud and swindling in online shopping, the Ministry of Post and Telecommunications has drafted this guide, jointly with other sectors and stakeholders, in implementation of public authorities' instructions aiming at reflecting the roadmap proposed by the national Authority for

preventing any ICT-related crime to curb this phenomenon.

The Guide is about the conceptual framework and hazards related to e-commerce. Besides, it highlights the provisions of e-commerce set forth by law 05-18 as well as the orientations to observe for a safe online shopping, in the one hand, and advice and orientations in case of swindling or fraud, in the other hand.

It is worth mentioning this guide was jointly drafted by the following sectors, institutions and bodies:

- Ministry of Post and Telecommunications,
- Ministry of Trade and Export Promotion,
- Ministry of Finance,
- Command of the Gendarmerie Nationale,
- Directorate General for National Security,
- Algérie Poste,
- Economic interest grouping (GIE Monétique).



I-Conceptual framework and hazards related to e-commerce





1. Basic concepts

In the light of the fast development of commercial transactions online in the past few years and the remarkable increase of purchase and sale operations online by citizens and commercial companies, public authorities have framed them by enacting law n05-18° of May 10th, 2018, defining the general rules of e-commerce. We hereby mention the basic concepts included in this text aimed for facilitating understanding the general framework of e-commerce, its parties as well as its legal and regulatory aspects.

- e-commerce:

According to article 6 of law 05-18, e-commerce is "the activity through which an electronic provider suggests or ensures the supply of goods or services remotely to an electronic consumer via e-communications."

- e-provider:

Any natural or legal person who shall market or suggest the supply of goods or services via e-communications.

- e-consumer:

Any natural or legal person who gets, either for a fee or free of charge, goods or services via e-communications from the e-provider for final use.

- e-communications:

Any correspondence, messaging or reception of signs, signals, writings, pictures, sounds, data or information of any nature, over wires, fiber optics or via an electromagnetic way. (Article 10 of law 18-04 defining the general rules of the post and e-communications).

- e-contract:

The contract, as defined by article 04-02 of June 23rd, 2004 related to the general rules applicable to the commercial practice, is concluded remotely without the real and actual presence of its parties, exclusively through e-communication technology.

- e-payment method:

It is a payment method authorized pursuant to the

regulation in force allowing to make the payment either up close or remotely, via an electronic system.

- e-advertising:

Likewise advertising, it aims, either directly or indirectly, to promote the sale of goods or services via e-communications.

- advance order:

A sale commitment which the e-provider may suggest to the e-consumer in case of a shortage of product in the warehouse.

- domain name:

It is a series of standard letters and/or numbers registered at the national register of domain names enabling to identify and have access to the website.

2. Main hazards related to online shopping:

Online shoppers encounter many hazards such as swindling and fraud. Some hazards are related to the software and equipments used in shopping, while others are combined to payment methods. Other dangers can relate to the process way and functioning of shopping in general. These hazards can be summarized as follow:

- the prevalence of pages and platforms offering high-demand and very competitive goods and services at lower costs, in order to rip off the consumer.

- the identity theft of e-shops shoppers or their credit cards and use of their personal data to buy online, bearing these cards real holders responsible for paying the costs of these goods and services,

- the import of goods that are not allowed to enter local markets,

- the risk of hacking e-payment cards and individuals' personal data, mainly through anonymous e-mails, fake websites, unreliable applications and software.

- the risk of dealing with anonymous agents due to the nature and specific feature of the virtual commercial transaction, likely to prevent having tangible proof if a complaint is filed.



**II-Guidelines about e-commerce transactions
pursuant to law 05-18**





It is about guidelines related to e-commerce transactions pursuant to the provisions of law 18-05 about e-commerce. The guidelines comprise the application of e-commerce, its conditions and requirement in addition to the rights and obligations of its parties.

1. Application of the law :

The Algerian law on e-commerce transactions applies in case any of the electronic contract parties is:

- of an Algerian nationality, or
- is a legal resident in Algeria, or
- is a legal person complying to the Algerian law,
- or if the contract is signed or implemented in Algeria,

Any transaction conducted via e-communications is not allowed if it is related to:

- Gambling, betting and lottery,
- Alcoholic beverage and tobacco,
- pharmaceutical products,
- goods affecting commercial, industrial or intellectual property rights,
- any goods or service prohibited pursuant to the regulation in force,
- any goods or service requiring the establishment of an official contract.
- sensitive products, materials or equipments defined by the regulation in force,
- any goods and/or services likely to affect the national defense, general order or public safety.

2. Terms and conditions related to e-provider

a)-Conditions of e-commerce practice

To be allowed to practice e-commerce, it is necessary to observe the terms and conditions defined in article 8 of Law 18-05, as follows:

- to register to the trade register or crafts and traditional industry register, as appropriate,
- to have a website or an online page, hosted in Algeria,
- to have the Algerian domain name: "com.dz",
- availability of the website on means allowing to verify its authenticity,
- to submit the certificate of obtaining the domain name to the national trade register center,

b)-Conditions of commercial transaction:

The e-commerce transaction is subject to the following conditions:

- anticipating the commercial transaction by an electronic commercial offer,
 - documenting the transaction by an e-contract,
 - the consumer's approval on the e-contract,
- Note: In case the provider does not respect these conditions, the e-consumer may ask for cancelling the contract and claim compensation for damage.

c)-Terms of electronic offer:

The e-contract must be readable and understandable. It shall also comprise at least:

- tax ID number, material and electronic addresses and phone number of the e-provider,
- number of trade register or craftsman's professional card,
- nature, features and prices of proposed goods and services taxes included,
- case of availability of goods or services,
- methods, costs and deadlines of delivery.
- general conditions of sale, mainly the clauses concerning personal data protection,
- conditions of commercial guarantee and post-paid service,
- price calculation method if it cannot be pre-defined,
- methods and procedures of payment,
- a full description of implementation steps of e-transaction,
- the offer's validity period if any,
- terms and deadlines of reversal if any,
- way of order confirmation,
- delivery date, price of product subject of prior order and prior-cancellation method if any,
- way of product return, its exchange or replacement,
- cost of using e-communications means when calculated on a basis other than the tariffs in force.

d)-Content of e-contract:

The e-contract must include:

- the detailed features of goods and services,
- terms and methods of delivery,



- conditions of guarantee and postpaid services,
 - conditions of e-contract cancellation,
 - conditions and methods of payment,
 - conditions and methods of product return,
 - methods of handling complaints,
 - conditions and methods of prior purchase order, if any,
 - conditions and methods of experimental sale, if any,
 - the competent legal party in case of dispute,
 - the contract duration as appropriate,
- Note: In case the provider does not respect these conditions, the e-consumer may ask for cancelling the contract and claim compensation for damage.

e)-Responsibilities and obligations of e-provider:

The contract signing entails responsibilities and obligations upon the e-provider as follows:

- after signing the contract, the provider is held responsible for the correct implementation of the commitments arising from this contract, either by him-self or by other service providers,
- sending an electronic version of the contract to the e-consumer after signing,
- establishing an invoice pursuant to the legislation and regulation in force, to be given to the consumer,
- return of the product by the consumer as it was when delivered in case the delivery deadlines were not respected,
- return of the product in case it was defective or not compatible with the order,
- order rejection if the product is not available in the warehouse,
- saving registers of achieved commercial transactions, their dates, and send them electronically to the National Trade Register Center (CNRC),
- collecting the necessary personal data to sign the commercial transactions, after obtaining the consumer's consent, by ensuring its safety and confidentiality.

3.Rights and obligations of e-consumer:

3.1.Rights of e-consumer:

- to have an electronic version of the contract after signing,
- to have an invoice delivered by the provider,
- to get a product conform to the purchase order, not defective, in the delivery date,
- possible return of the product as it was when delivered, in case the delivery deadline was not observed, or if the offer supply was defective or not compatible with the order.

3.2.Obligations of e-consumer (Articles 16-17)

- to pay the price agreed upon in the e-contract once signed, unless otherwise defined in the e-contract,
- to sign a receipt in the real delivery of the product or performance of the service subject of the e-contract,
- a copy of the receipt must obligatory be delivered.

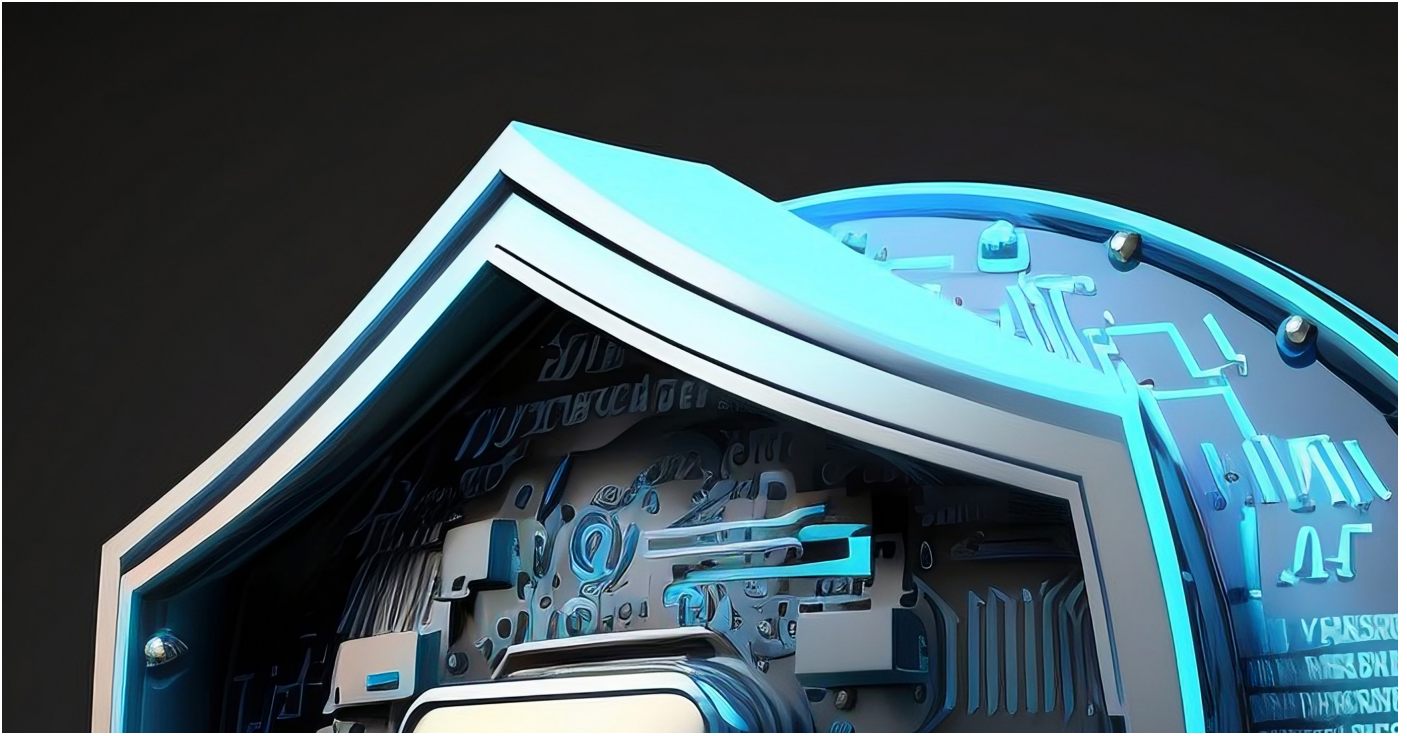
4. Payment in e-transactions:

In the e-transactions, the payment shall be either remotely or while the product is delivered, via the payment authorized means, based on the legislation in force.

When the payment is online, it is conducted via specialized platforms created and used exclusively by authorized banks by Banque d'Algérie (Algeria's Bank) and Algérie Poste (Algerian Post corporation) connected to any e-payment stations via the public telecoms network. These platforms are subject to the monitoring of Banque d'Algérie to ensure its response to the interoperability requirements, data safety and confidentiality in addition to the safe exchange.

In the commercial transactions oversees, exclusively remotely, the payment shall be via e-communications.

The receipt of the e-provider website must be safe via an electronic authentication system.



III-Guidelines for a safe shopping online





It is about guidelines to raise the awareness of providers and consumers of any shopping transaction online, which makes the online shopping safe.

1. Use of reliable antivirus software

The download and installation of official and reliable antivirus software, from official websites or certified suppliers, on computers mainly those usually related to e-commerce (computers, smart phones and tablets), its regular update ensures a safe e-commerce for the user either as regards making calls, exchanging messages or shopping online.

2. Use of reliable applications:

It is recommended to download applications specific to smartphones and tablets from official and reliable sources only, such as (App Store) for (iOS), (Google Play) for (Android) or (HUAWEI App Gallery) for (HarmonyOS). It is also suggested to see comments about applications' stores to get informed about other users' opinions. Besides, the installed applications need to be updated on equipments either automatically or manually from the download store.

3. Use of a strong password:

It is suggested to use strong and complicated passwords including a mix of letters (capital and small), numbers and symbols as well as to avoid frequent words or those concerning personal information or a simple set of figures or letters. Using the same password in all websites, accounts and applications must be avoided to prevent being hacked and personal information to be disclosed.

The passwords should be modified constantly, and are not to be shared with others.

4. Activation of 2-factor authentication:

The "two-factor authentication" is an automatic extra option to protect accounts especially when the password is hacked. It can be acti-

vated to prevent anyone from having access to the account. The account owner can log in with a password that can be transmitted to the mobile phone.

5. Preservation of personal data:

In this regard, it is highly recommended to attach great importance to the issue of the preservation and non-sharing of personal data and avoid sharing personal data particularly those relating to payment cards and personal accounts.

6. Modification of default settings on the user's tool:

The default settings of the user's account or internet surfer must be checked and modified to avoid saving the data of login, e-payment, postal or bank accounts.

7. Staying cautious about dealing with emails, contacts and adverts

In this respect, it is recommended to stay cautious about:

- spam and activate its deletion,
- misleading messages like: "Hurry Up The Limited Offer", "login and win prizes", etc.
- fraudulent messages: aiming at ripping off consumers.
- warning adverts: it is recommended to read them carefully and deal with them cautiously.
- fraudulent calls: from fake tradesmen having fake websites.

8. Use of safe tools, websites and networks:

In this regard, it is suggested to avoid using general tools and rather use personal tool while shopping online in a bid to protect the personal information and financial account data.

It is also recommended to avoid registering personal data and postal or bank card data on a general tool connected to the internet.

Before any online shopping, it is necessary to make sure the website starts with (https://) rather than (http://), i.e. the websites are protec-



ted with reliable coding protocols.

9. Consulting shopping website terms and privacy policy:

In this regard, it is recommended to consult:

- The privacy policy which is a set of terms and conditions clarifying the way of collecting, using and exchanging the personal information of the website visitors,
- the buyer's name and products offered online,
- other users' assessments and comments about products to make sure about the product's quality,
- the policies of return and refund,
- the existence of a payment receipt,

10. Confirmation of the product's nature and verification

Before choosing the product, it is necessary to make sure it is not prohibited goods from import and transaction. As delivered, the product must be carefully verified to make sure of its expiry date and safety pursuant to the terms agreed upon with the buyer.

Secondly: Guidelines related to payment method:

- It is necessary to know the emergency number of the bank or financial institution or contact centers.
- putting payment cards in a safe place,
- avoid saving the card's password on the computer, electronic accounts or sending it via emails,
- avoid saving the password with the card together to prevent any fraud risk,
- avoid sharing the password with anyone even if he were trustworthy, including consultants of

postal or banking institutions.

- audit of financial accounts regularly to make sure there is no suspicious activity and contact the postal or financial institution of the user in case of any fraudulent operation online,
- activation of text messages related to the postal or bank accounts to enable the user to be informed and warned about any financial transaction conducted on his account.
- to make sure about connecting the payment card with the mobile phone number of the card's holder, and to modify it if lost or ceded to avoid the eventual confirmation of payment sent via SMS by another person bearing the old number line.
- In payment step, it is necessary to make sure the new payment window offers one of the following addresses:

<https://epay.poste.dz> or <https://cib.satim.dz>, otherwise do not register your data.

- Required information in payment process via the card:

- the card number comprising 16 figures,
- expiry date,
- protection and safety symbol on the back of the card comprising 3 numbers,
- Name and surname,
- prior to payment confirmation, it is necessary to see if the transaction amount included or shown on the payment page complies with that of the offered product on the buyer's page,
- avoid saving personal data of payment card on the commercial site,
- If the payment card is lost, it must be blocked immediately by any possible means (call centers, post offices, bank agencies, money applications, etc).



IV. Guidelines stemming from registered swindling and fraud





According to the field preview by safety departments and other stakeholders involved in the e-commerce transactions in Algeria, commercial transactions have been conducted online and citizens believe it is about e-commerce via social media and other websites, but indeed, these transactions do not meet the requirements and terms of e-commerce as stipulated in law 18-05.

Besides, there are several websites, pages and platforms offering goods and services to consumers, highly-demanded and with very low prices, very interesting offers, in a bid to swindle citizens in view of the widespread use and diversification of swindling and fraud ways about shopping online.

We hereby tackle the key ways of registered swindling and fraud, and then suggest preventive guidelines to adopt in case of swindling or fraud.

A) Main ways and methods of swindling and fraud :

The most frequent swindling and fraud operations in Algeria relate to social media websites by fake shops activating outside the legal framework that defines e-commerce. On some electronic pages, highly-demanded goods and services with very low prices and very interesting offers are portrayed to rip off the shopper knowing that the swindler receives amounts of money in advance on his postal or bank account or through money transfer service available in phone applications of financial institutions, without sending the product to the applicant.

Swindlers and fraudsters use several techniques and methods to rip off citizens while conducting online shopping. These techniques can be summarized as follows:

-Pages imitation: it is used by the fraudster to deceive the consumer and convince him of communicating with known and reliable parties or legitimate electronic suppliers;

Urgency: The fraudster uses it to deceive the consumer by highlighting the importance of the offer and its short duration, making it urgent to imply to the fraudster's request He may ask him

to send money, provide personal information or click on harmful links;

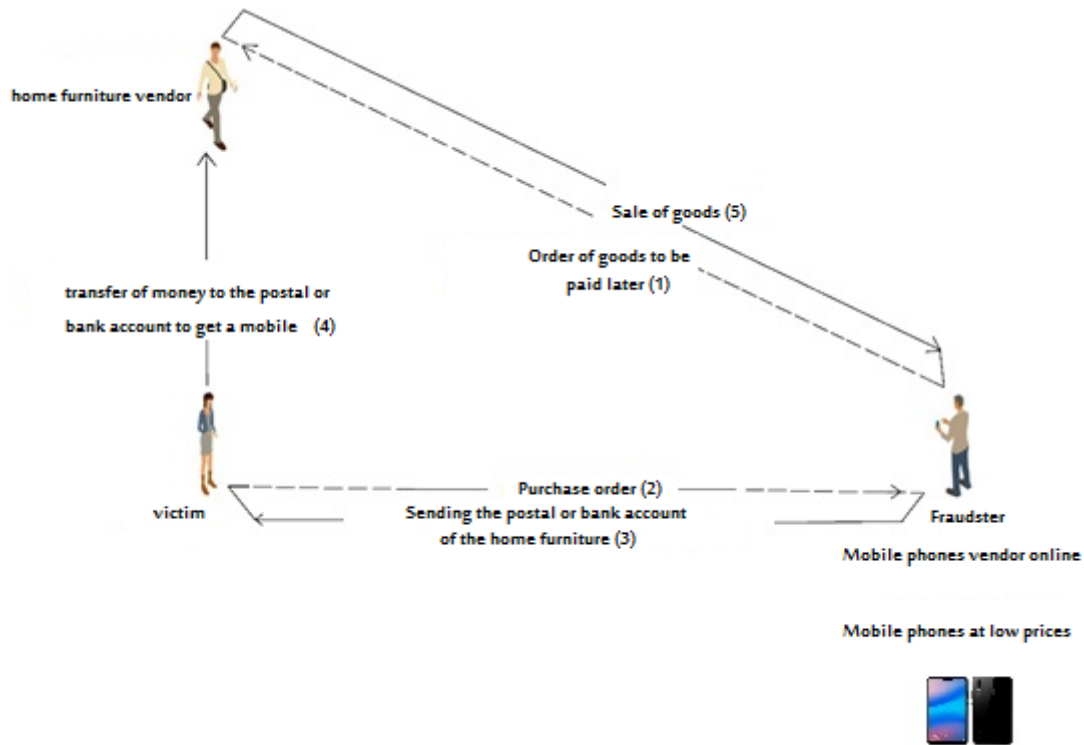
-Emotional manipulation: this method aims to manipulate the consumers' feelings and emotions to persuade them to obey fraudsters' requests such as sending money or buying a product,

- Forgery and fraud via misinformation: This process relates to the impersonation of Algérie Poste Corporation to fault victims via fraudulent short text messages bearing the name «ALG Poste» confirming payment in their postal accounts in order to prove payment for sales or confirming settlement of commercial transactions performed remotely.

Fraudulent messages sent to victims' phones are similar in content and form to those actually sent by Algérie Poste Corporation (AP) to its active customers for the account tracking on the phone. Fraudsters use international electronic websites and platforms providing SMS worldwide, exploiting the possible falsifying of the sender's name and adopting AP's name in a bid to delude their victims that the SMS verily stems from AP to inform them about money transfer into their accounts.

Fraud triangle: it is about three parties: the fake seller (fraudster), the real seller (victim), and the buyer (victim). It goes through the following stages:

- The fraudster initially purchases goods or service from the real seller and both agree that payment is conducted via a bank or postal account.
- Here, the fraudster offers the goods or service via social media sites, and agrees with the buyer (victim) to send the amount of the fictitious product via a current postal or bank account, which should be that of the real seller;
- After confirming the buyer has paid the agreed amount of money, the fraudster blocks the latter on all social media platforms and then disappears after implicating the real seller with the buyer (victim).



B) Guidelines about the attitude to adopt in case of swindling or fraud

In case of being a victim of swindling online, it is recommended to stay calm, although feeling angry or frustrated is a natural attitude, it is important, then, to take the following measures:

- to collect as much information as possible about the fraud, including the transaction's details (the fraudster's account, the amount of money, the exchanged emails, screen shots, the website's or page's links, ...),
- to head to the closest security post (police or national gendarmerie based on the regional jurisdiction) to report on the fraud with electronic media and information collected about the transaction,
- If it is not possible to head for safety department, the victim can report it via the toll-free number 1548 (police), 1055 (national gendarmerie), 3311

(consumer protection associations), 1020 (Ministry of Trade and Export Promotion), or via the links of the national safety departments:

-Algerian police : contactccp@algeriepolice.dz

-National gendarmerie: https://www.mdn.dz/site_cgn/sommaire/services/ppgn/ppgn_ar.php

-It is also possible to submit complaints to the relevant departments of the Ministry of Trade and Export Promotion.

-to report on the websites and social media pages of the security departments, any account, page or publication of swindling for blocking and preventing others from being a victim of it.

-to freeze payment cards mainly in case personal data has been stolen or in case of any doubt about a swindling transaction.