MODULE 3: Customer support, privacy and security in E-Commerce

E-entrepreneur

STRATEGIC PARTNERSHIP IN THE FIELD OF YOUTH

Project ID: 2019-2-DK01-KA205-060317

Funded by the Erasmus+ Programme of the European Union

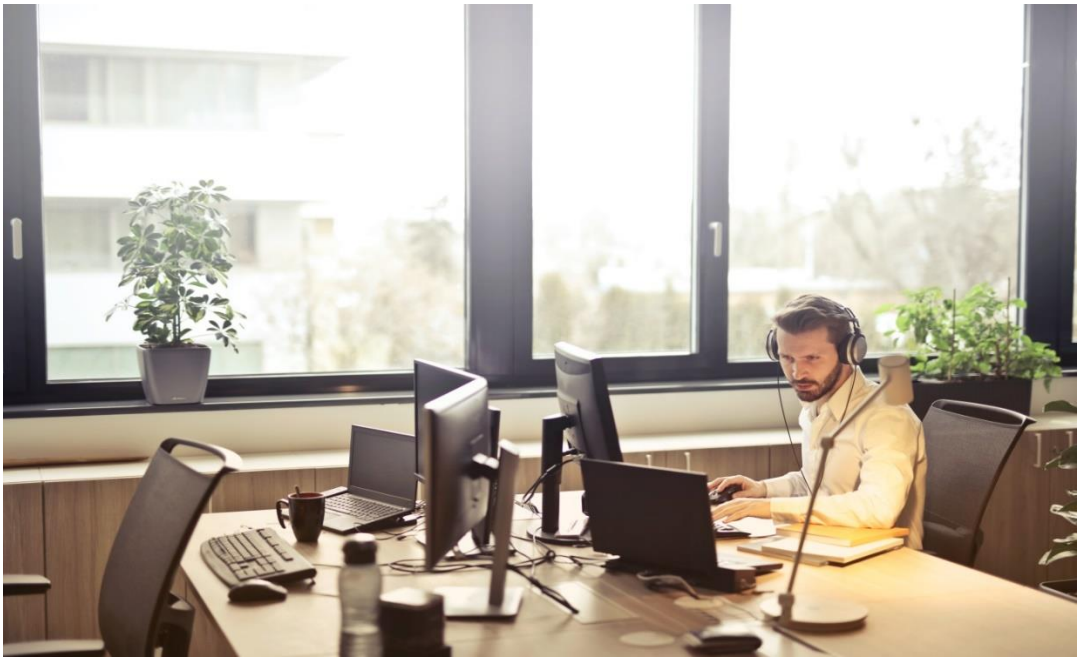
This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CONTENTS:

INTRODUCTION

Engaging in E-Commerce is not as simple as we believe, there are dangers that can and must be avoided. Thanks of this module, youth workers, educators and young entrepreneurs will understand what are the dangers for any user, whether it is a buyer or a seller. We will analyze what are the factors related to privacy and security in a shop and the related tools used to guarantee users maximum protection.

Another fundamental element is customer service, a tool that is the basis of a successful E-Commerce; we will see which are the factors to be developed to offer customer an effective and efficient service, precisely to create customer loyalty.



THE IMPORTANCE OF CUSTOMER CARE

We live in a world governed by super competition within saturated markets and therefore the only way for young entrepreneurs to have an advantage over others is to create a relationship with customers as much as possible. This applies both to physical activities, but even more to E-Commerce, where competition increases day by day.

If in the past years it was enough to have the best product to be able to successfully appear in a market, today this is not enough. Each company must create a relationship with its consumers and this relationship passes, yes, from the Brand Identity management, but also from the care of the pre and post-sale assistance service.

Entrusting customer care to qualified personnel is a basic requirement for any entrepreneur that wishes to create a long-term relationship with the consumer (retention) and make sure that he or she can buy again as well as he or she can recommend its products to the acquaintances, activating that advocacy and word of mouth process that every business should aim for.

Among other things, a drop in the quality of customer care is also an indication of a general deterioration in the performance of a business.

Taking care of your customer means having the future of your E-Commerce at heart and putting the consumer at the center, it means understanding your needs, and being able to find the system to satisfy them.

At the base of all this is customer support, those who buy on the internet have a thousand questions, because they cannot physically see the product. A young person who wants to become an entrepreneur in E-Commerce must focus on this if he or she wants to win the competition.

CUSTOMER SERVICE

The difference between a positive and a negative comment is sometimes given by the promptness with which the customer service is able to assist the customer. Many E-Commerce offer contact through different ways among which we can distinguish:

- telephone contact;
- chat contact;
- contact by email;
- contact via social profile (Facebook page mainly).

The presence of telephone contact is a distinctive and "comforting" feature for the customer who decides to make a purchase, especially of a high amount, as he or she knows who to contact immediately in case of any problem. The availability and competence of the telephone operator are essential for a good evaluation by the buyer. It is important to offer a free telephone line as the paid ones will create "friction" in the purchase decision. This typology is mainly exploited by adults.

Customer service via chat is spreading: by opening the page of an E-Commerce site a window, usually in the lower right corner, allows immediate contact with a company operator to receive information on the product to be purchased or on other aspects little known. It is normal for young people who shop online to be more likely to ask for information via chat, which is why most E-Commerce sites rely on this type of assistance.

CUSTOMER SERVICE IS THE STRENGTH OF AN E-COMMERCE

The great E-Commerce[1] have focused on customer service to increase their strength and their reliability, this also applies to those who are now approaching this business. What to focus on, what are the aspects to be developed to offer a complete service? More and more young people are trying to become e-commerce entrepreneurs, but these must know what to focus on to be successful. What distinguishes efficient customer service from one that doesn't work?

Short response time

Having the best customer service in the world is not enough if young entrepreneurs answer after whole months, because the one who was willing to buy, will never be seen again! Nobody likes to wait and, in a world that is now at the speed of light, a customer service must guarantee maximum response speed.

Unlike an offline store where someone has questions or concerns physically goes and has an answer, the online store cannot guarantee this. Hence, customer service

[1] We can take Amazon as an example, today the first company in the sector for revenues, amounting to almost 233 billion dollars from which a net profit of over 10 billion dollars.

becomes the only way to establish a relationship with the potential customer. It is for this reason that you cannot keep days waiting when a customer writes by email or chat, indeed, you must ensure an immediate response.

Most E-Commerce businesses makes the section dedicated to requests clearly visible, this to testify even more the importance; the prospect doesn't have to waste hours just to find ways to get in touch. The most organized have three specific categories: one for customers who have already ordered and need after-sales assistance and are looking for information regarding the delivery status, return or problems relating to the product already received; one for customers who have difficulties in the order phase and, finally, a category for those who are in the pre-order phase and would like details on the items. This is because, those of competence will have a clear scheme on where to direct the customer and also allows you to dispose of all requests faster.

- **Team always updated**

Customer service that is not constantly updated is not professional. In E-Commerce those who deal with customer service must be able to respond to a request as quickly as possible, without having to do specific research while on the phone because they do not know what the customer is talking about. In practice, in addition to knowing every item in the shop's catalog from top to bottom, you need to have the technical skills to help the customer "at a distance". In addition, the customer cannot know the technical language that is normally used in the company: for this reason, the customer service team usually must have the ability to understand the problem that is hidden under words that are sometimes very simplistic.

It is not easy for customer service staff to know every single millimeter of the E-Commerce store to perfection, especially if the items are constantly updated and there is always a lot of news. This is why companies are constantly organizing training courses, which may be demanding in terms of time and money, but the result is customer satisfaction, which will be faced with staff trained on several fronts.

If we talk about a large electronic shop that spans several sectors, the staff is divided. This is why, if the team is made up of a large number of customer service staff, it is divided according to their skills.

- **Clear and concise communication**

It is useless to have a super competent and prepared customer service, if he or she speaks only in technical language, which is unclear to who is on the other side of the phone or computer screen and if it takes years to explain a concept. For this reason, the E-Commerce team always uses clear and concise communication.

Communication must be concise because when you answer a customer, the minutes are counted. This is because, as a rule, there are many other requests and you cannot afford to miss half a day for every single person who gets in touch. This is why, both by email and by phone, it is essential to fully understand what the customer is requesting and to provide a short but effective response.

Furthermore, the type of communication must be clear and transparent. Honesty and empathy are the best qualities of those who deal with the customer service of an E-Commerce: no technical words that an ordinary person cannot understand, but simple words and a natural and colloquial language. The important thing is to never lose patience, this distinguishes effective customer service from ineffective one.

- **Always use positive language**

The customer service of an E-Commerce store always uses positive language. This is because when a customer contacts he or she does not do it to waste time, but because he or she needs support. Starting from this awareness, it is important that extremely negative answers do not fall upon him/her. It also affects the image and the brand.

There may be situations where the problem does not depend on the company, for example, when it is the external company that deals with shipments that delays the delivery of a package, and, in this case, the only thing that matters is to be available , kind and helpful to customers, because it is in these cases that it is seen if a customer care works. This is why complaints must be accepted, and also because they can be useful for improving the e-shop and the service.

- **Not just a toll-free number**

Most electronic stores, or rather the larger ones, offer customer service on various channels, and therefore not only by telephone. The company works to understand what the customers' needs are, so it makes available all the means to respond to these problems. A toll-free number is available to a mainly adult audience, as well as e-mail. If, however, your target refers more to young people, you opt for the chat on the site.

As for Social Networks, being present with a company chat on Facebook is important, as, to date, it is one of the most used ways for customers to get in touch with a company. This is because it is also an immediate tool. In this way, customers are covered at 360 degrees.

WHAT BENEFITS AN EFFECTIVE CUSTOMER SERVICE DOES

Naturally from this analysis it turns out that a competent customer service brings countless benefits to E-Commerce, and it is obvious that whoever wants to become an online entrepreneur must keep in mind that this is a fundamental service to be successful.

An effective customer service allows you to better welcome the customer in the business and to almost completely flatten the difference with the physical store. As, in fact, in a physical shop you raise the shutter and entertain the public, a competent and friendly customer service team in E-Commerce allows you to open the doors to visitors: when someone has a question, they respond in a polite and polite way in every moment, just like it would happen by consulting a job within a common offline store. This allows you to create credibility and professionalism around the brand, two fundamental characteristics for an E-Commerce: people, especially if they are not used to buying online, need human contact, to speak with someone who can respond to their requests, to be continuously reassured.

A customer service is thought out in every detail and allows increasing sales: responding carefully to pre-order requests leads to greater satisfaction and conviction in the user, who will therefore be driven to buy. Subsequently, having found himself at

ease, he or she will return over and over again: at this point, the company reaches customer loyalty.

It turns out, therefore, that an E-Commerce has everything to gain and nothing to lose to make its customer service effective, which, if exploited to the maximum, can truly become a strong point for the business: most shops Electronica does not pay particular attention to a customer service that responds promptly and optimally to customer requests and, sometimes, confusion is the master. Whoever offers quality customer service differs from the competition. The concern for the customer comes first and always leads to excellent results!

COMPULSIVE ASSISTANCE: CONTRAINDICATIONS[2]

However, there may also be contraindications. The responsiveness to customer responses, if on the one hand, can be included among the so-called factors. "Motivating" who can push the purchase of a good or service on the other hand can create spoiled customers in e-commerce who, by now accustomed to this service, see this factor as "hygienic" (Herzberg, 1959).

In recent years, this change has led to a change in a part of the clientele which today is more than demanding, unaware of the limits and the functioning of the E-Commerce activity itself. Some sellers see calls and messages delivered even in the most unlikely hours of the day and admonitions from customers if the answers to their requests do not take place immediately. This phenomenon is typical of e-commerce in that in traditional retail activities a buyer would never contact the seller outside of opening hours, also because no one could answer on the other side of the phone.

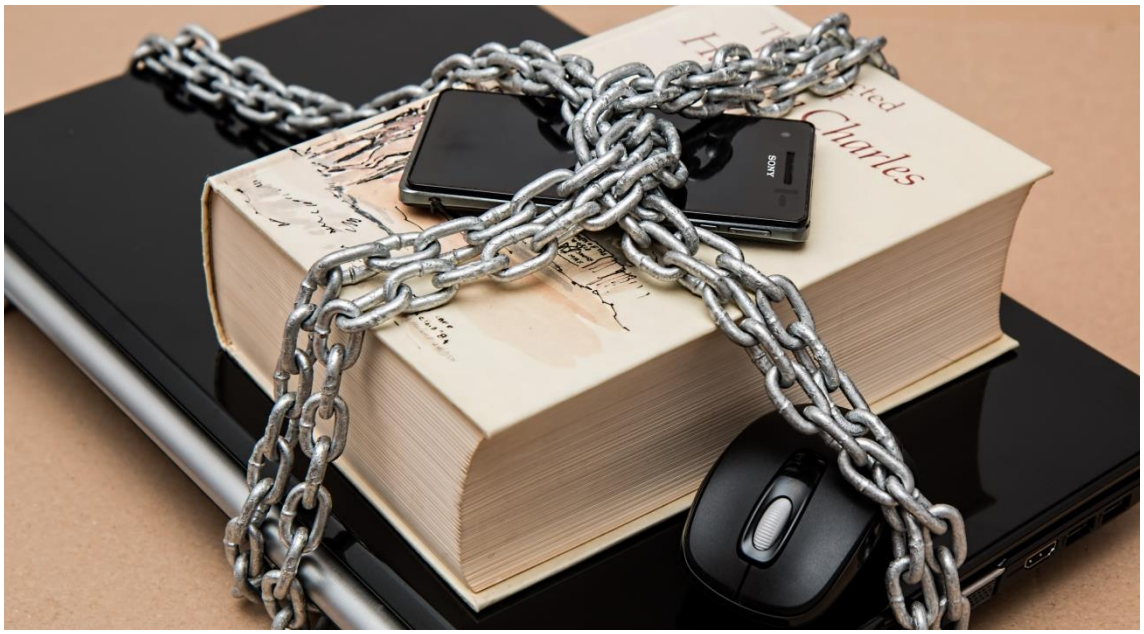
[2] Working as a customer service agent is not easy. Most operators feel stressed and overworked, so much so that 35% consider changing job.

THE IMPORTANCE OF PRIVACY[3]

When it comes to E-Commerce, protecting consumer privacy and being transparent about business practices is a matter of respect. It is important that customers understand exactly how their data is used and whether they have control of their personal browsing information.

With a large number of devices that collect and share information in constant growth, consumers are increasingly interested in how their data is collected, used and protected. When it comes to their digital privacy, they are afraid of being exploited, harassed or damaged by the exposure of their digital data, but a recent Harvard Business Review study shows that many consumers don't even realize the type and importance of personal data that spread online.

Although the collection and use of data is important for E-Commerce companies so that they can offer experiences with personalized and relevant ads, it is even better to implement this transparently.



[3] *The eleventh commandment - do not let yourself be discovered - is the only one that is practically impossible to respect in these times*.
(Berthe Henry Buxton)

Among the key elements of a relationship of transparent privacy and trust between customers and merchants there is an explanation of what data is collected and which is not, as well as the ways in which this affects the online experience of a surfer. An option of easy access and use for voluntary renunciation can be added, with a language that explains how this affects the advertising experience of those who surf, and perhaps easy access to a complete privacy policy, as well as information on any industry standard or privacy commitment adopted by the company.

Why it is important to provide privacy information

The data controller takes the appropriate measures to provide the data subject with all information relating to the treatment in a concise, transparent, intelligible and easily accessible form, in simple and clear language, in particular for that information intended for minors. The information is generally provided in writing or by other means, including through electronic means. There is nothing to exclude that this information may be provided orally, at the request of the interested party and provided that the identity of the interested party is proven by other means. The European legislator has taken compliance with the transparency obligations very seriously, by providing, on the one hand, the responsibility of the owner (and manager).

But what information must be provided

At the time when personal data are obtained, the data controller is obliged to provide as personal data:

- the identity and contact details of the data controller or possibly of its representative, i.e. the natural or legal person that is designated by the data controller or by the data controller representing them;
- the contact details of the possible data protection officer (DPO), as a contact point also with respect to the interested parties;

- the purpose and legal basis of the processing and any recipients or any categories of recipients of personal data;
- the retention period of personal data or, if not possible, the criteria used to determine this period;
- the existence of the right of the interested party to request the data controller to access personal data and to correct or cancel them or limit the processing of data.
- it is very important, if the treatment is based on the consent expressed by the interested party, the right to withdraw the consent at any time;
- the right to lodge a complaint with a supervisory authority, this can be considered one of the fundamental rights, especially for a customer of an E-Commerce store who has more limitations in checking for example the validity of a goods, compared to the customer of a physical store.

All these conditions, which must be indicated in the privacy policy of an E-Commerce, are:

a) the existence of a Commission adequacy decision;

b) in the absence of adequacy decisions by the Commission, the reference to adequate guarantees that must be provided by the owners involved and an indication of the means to obtain a copy of these guarantees or the place where they were made available;

c) in the absence of any other assumption, the reference to the conditions, applicable in specific situations, such as the explicit consent of the interested party, who has received all the necessary information on the risks associated with the transfer.

Data retention time

The data that refer to the processing of an E-Commerce contract will be kept for a period not exceeding that necessary to achieve the purposes for which they were collected or subsequently processed and, in particular:

- the data provided by sending e-mail messages or filling in the contact forms on the site will be kept for the time necessary to provide feedback;
- the data provided for a subscription to the newsletter service will be processed until requested by the interested party to cease;
- the data provided by filling out the form in the "work with us" section will be kept for a maximum period of twelve months from their conferment and may be used for any contacts aimed at subsequent selections;

The Data Controller of the shop will, after the expiry of the retention periods according to these criteria, delete or possibly anonymize the data that should not be kept for specific regulatory obligations.

What to do with the data collected for a different purpose

If the data controller intends to further process personal data for a purpose other than that for which they were collected, he or she must provide the interested party with further information:

• indication of the new purpose;

• retention period of personal data or, when the criteria used to determine this period is not possible;

• any decision-making process based solely on automated processing, logic used and consequences for the interested party;

• rights of the interested party: access, rectification/integration, cancellation, limitation, opposition, portability, complaint to a guarantor Authority, withdrawal of consent in cases of law.

A fundamental prerequisite for an E-Commerce activity is the adoption of a privacy policy that respects what has been described so far. Today it is very easy to find someone's personal data, especially for those who use electronic tools, which is why first of all must be those who request the data to avoid the dissemination of the same.

Ensuring the privacy of a customer, for an E-Commerce store, but not only, means laying the foundation stone for a solid relationship of loyalty between the store and the customer.

THE SECURITY PROBLEM

The Internet offers opportunities for communication, information and a wide range of unthinkable services but all this conceals risks related to e-commerce, the possibility of falling victim to computer crimes or the loss of the confidentiality of one's personal data.

The risks of e-commerce stem mainly from the fact that full consumer protection appears difficult to achieve, especially if you decide to buy abroad where different regulations apply. And this is undeniable when buying goods that have not been physically seen by a seller who has never known each other and who, if there are problems, does not have a shop under the house to go and claim. Online commerce opens up new forms of crime such as the theft of credit card codes or the violation of access and use of sensitive data. The main dangers come from scams, intended primarily in an attempt to steal money, so it is important to know what the payment methods in an online store are and how they work and what are the "pitfalls" that are used, to know how to defend you.

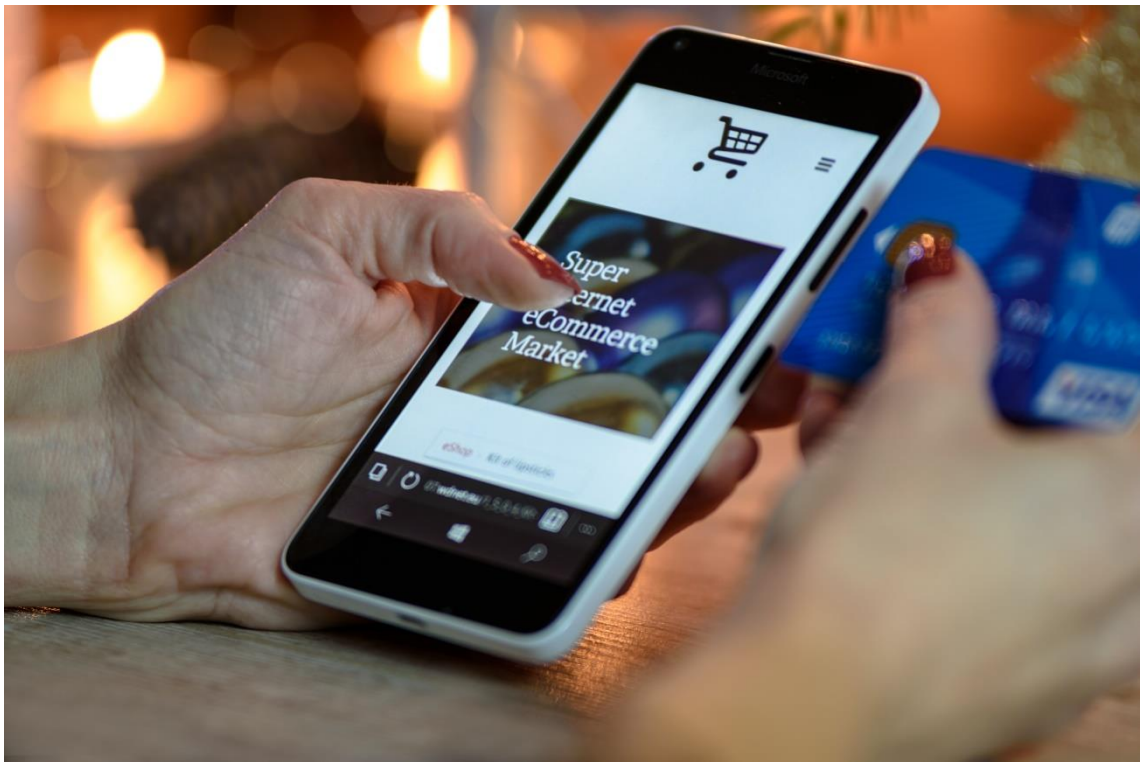
PAYMENT METHODS AND SECURITY

One of the most felt problems in the world of E-Commerce is undoubtedly the security of the payment method. To date, the most common methods are bank transfer, cash on delivery and payment by credit card. Initially, the transfer of information and personal data between the seller and the customer took place in the clear. This was a huge security concern, as the transferred data were easy to intercept and then used by third parties to carry out fraud. For this reason, people still believe that this way of purchasing goods and services is insecure or exposed to risks.

In particular, most E-Commerce sites today use high levels of encryption such as, which make the transfer of money and data very secure. Eg:

- Transport Layer Security (SSL/TLS). The combination of this protocol with normal HTTP allows obtaining a new protocol: HTTPS. It guarantees the sending of personal information in the form of encrypted packages in this way, the transmission of information takes place in a secure manner, preventing intrusions, tampering and falsification of messages by third parties. An encrypted communication channel is created between the client and the server through an exchange of certificates. To accept https connections, the web server administrator must create a digital certificate or an electronic document that associates a person's identity with a public key. The authentication process verifies that the applicant has administrator permissions for the domain for which the certificate is being requested. The HTTPS protocol does not guarantee the confidential transmission of data, but their integrity. The pages protected by this protocol are easily recognizable, as the word "https" precedes the address of the protected site and its pages are marked with a padlock, which can be viewed in the lower part of your browser.
- "User authentication" procedure. Generally, this procedure occurs by requesting a username from the server with which a password is associated. However, this system cannot be considered completely secure, as the time it takes for third parties to find the password is increasingly reduced.

- The seller as well as the consumer must also be protected. One of the main problems that affect the seller is that the buyer arbitrarily decides to withdraw from his purchase. To cope with this problem, the digital signature is used which means that a digitally signed contract cannot be denied by those who have signed it.
- Another fundamental point is the care of internal security, that is the security and maintenance of the server where the E-Commerce structure resides, whether it resides at the company or at the server of a hosting company; in fact, there are criteria and guidelines to be respected for server security, to naturally guarantee data integrity.



PASSIVE SAFETY: CAPTCHA[4]

The term “captcha” defines small windows containing a sequence of distorted or blurred numbers or letters. The purpose of the captcha is to automatically determine

[4] completely automated public Turing test to tell computers and humans apart

whether to make a registration, login, or other action on the internet, is a human being or a bot. This procedure is an insurmountable obstacle for spam software, only one person can discern individual letters or numbers from such an encrypted design.

It compares the value of the text box in which the user entered the values with the content of the session variable created before, offering a positive or negative result depending on whether the condition is met or not. That's why this is considered to be one of the best security systems on the internet.

ONLINE PAYMENT SYSTEMS

With the expansion of electronic commerce, new problems emerge related to the transposition of traditional means of payment in the new context and also the need for new means of payment, capable of satisfying the security and authentication needs that an online transaction on an open network It expected. The use of cryptography and its applications (digital signature, for example) certainly represents a valid response to these needs. But providing your data or your own credit card does not guarantee neither a correct payment security, nor a guarantee for who receives the payment. The only viable way to protect users and citizens is to store all the information necessary for the traceability of purchases (IP, Log file User registration, address of delivery of the goods, contact information with the customer) these data, if stored, will be useful to the competent authorities for the identification of the perpetrators of the crimes, relying on the fact that they are almost always identifiable. Furthermore, post-sale data retention is also necessary in the case of an abusive copy of the credit card number and CVV or CVC code, the owner becomes aware of the fraudulent transaction, very often, only at checking the account statement, delaying the reporting time of the crime event greatly.

The development of online commerce has inevitably led to the introduction of new digital payment systems. In recent years, several internet payment tools have been created and many of these require the intervention of a third party as an intermediary. Depending on the type of instrument used, the intermediary may be linked by a

contractual relationship to the buyer, the seller or both. The main electronic payment methods to date are:

Credit card

The main payment method for online transactions is definitely the credit card. This type of payment requires the customer to send the credit card details to the seller. Subsequently, the same seller transmits the data to the bank by initiating a verification and credit procedure. Transactions are debited to the current account in arrears, usually in the middle of the month following the purchase. Of course, also in this case the transaction takes place in a secure way, as the data are known only to the recipient and not everyone.

Wire transfer

At the end of the transaction the seller's site communicates the bank details to which to make a bank transfer for the amount of the goods. Upon receipt of the transfer, the seller sends. A problem, in this case, could concern the longer technical times for making the transfer. These problems can be solved with web banking.

Mark

This form of payment is the one that provides the least risk, since payment is made only once the goods have reached their destination.

PayPal

It is the eBay group company that allows anyone with an e-mail address to send or receive payments online easily, quickly and securely. The operation of PayPal is very similar to that of a common bank account, after opening the account you can send or receive money and make payments online. This system is frequently used on eBay or in many online stores, as an alternative method to a credit card. To date, perhaps it is the most used method precisely because it guarantees a fast but above all secure payment.

Prepaid cards

These are cards that can be purchased with a fixed amount available, as is the case with telephone cards. With these cards it is possible to buy via the Internet. The advantage over the traditional credit card lies in the fact that, in the event of abuse, you are sure that the damage suffered cannot exceed the value of the predetermined card. For this reason it is advisable to buy prepaid cards with a not very high value.

MAIN TYPES OF ATTACK

As mentioned above, the SECURITY issue on the internet is very delicate, as there is always someone trying to steal data and money. And the bad thing is that you don't know who's on the other side, that's because it uses different scam methods. Of course, technology allows you to defend yourself from these attacks but it is always better to know what these scams are, this is especially true for those who, like young people, approach the online market for the first time, but not only.

Phishing[5]

It is one of the best known and most used techniques to finalize identity theft as it consists in the use of electronic communications, especially fake e-mail messages, to find information relating to the victim user.

The content of these e-mails often contains links to bogus sites, consisting of pages very similar to those of the real site in order to deceive the user by making them insert sensitive data on special forms. This type of activity, while still being widely used and effective, is giving way to a new technique that has been gaining more and more value in recent years: vishing. Vishing is a particular type of phishing that is based on voice communication, that is, through phone calls to the victim.

Pharming

This is a cracking technique, used to obtain access to personal and confidential information, with various purposes. Thanks to this technique, the user is deceived and led to unknowingly disclose his sensitive data to strangers, such as bank account number, username, password, credit card number and many other data. The ultimate goal of pharming is the same as phishing, directing a victim to a "clone" web server specially equipped to steal the victim's personal data. To defend against pharming there are still no specific programs except firewalls that try to prevent access to your PC by external users and antivirus programs that block the execution of malicious code.

Firesheep

Even more dangerous, since it can be used by anyone, it does not require any specific computer knowledge. Firesheep is a Firefox add-on that makes identity theft extremely easy. This extension "captures" the login credentials of users present on the same network, and with a simple login the corresponding cookie is captured and makes it available for access in a convenient browser sidebar. Firesheep takes advantage of some bugs on websites, such as Facebook, Amazon, Twitter and many

[5] Even in 2019, most hackers attempted attacks using email as their primary channel, especially to carry out phishing campaigns.

others. To retrieve active sessions, which travel in the clear, use a special script. Some sites, subject to these attacks, have taken shelter by using secure connections using HTTPS during the transfer of cookies.

Denial of Service (DOS)

Another type of attack, frequent on the web and in particular against sites dedicated to E-Commerce, is the DoS (Denial of service). The attack is conducted through networks (botnets) made up of so-called zombie computers, which by connecting to a website at the same time overload it, making it unusable. The owners of the computers involved are often not even aware that they are part of the botnet (the set of infected computers), which makes defense much more difficult.

This type of attack is normally used to discover flaws in the E-Commerce site, in order to retrieve information on users who connect, in particular access credentials and credit card numbers.

Keylogging

A keylogger is a tool that can intercept everything a user types on the keyboard of their computer.

There are two types of keyloggers: hardware, they are connected to the communication cable between the keyboard and the computer or inside the keyboard; software that are programs that control and save the keystrokes that a user enters.

Hardware keyloggers are very effective because their installation is very simple and the system is unable to notice their presence.

ONLINE SCAMS

Purchases on the internet represent the 2.0 store and are very comfortable but at the same time involve a high risk of running into an online scam, especially in e-commerce sites and auctions between individuals. An online scam occurs mainly through sending e-mails and links to fake sites. As for e-mails, their main objective is to steal the user-

password pair from the user, in particular the credentials of banking services present on the web, so that they can access it and make a money transaction on other accounts currents.

Sometimes, instead of forwarding the user to a bogus site, they expressly ask to reply to the e-mail by providing their credentials by pretending a fake failure of the IT system of the web service to which the user refers.

Other types of scams have to do with E-Commerce sites, where the scammer just needs to create a website with false data and start selling products at very advantageous prices. This type of site hides a so-called ghost shop, because after purchasing the product it is never sent and the shop disappears.

HOW TO PROTECT YOURSELF

Being completely safe on the internet is difficult, but knowing how to protect you is a fundamental thing. As for phishing sites, you need to pay close attention to the URL present in the web browser in order to immediately check if you are connected to the right site. Before making an online payment, especially on an unknown seller, you must first check whether the VAT number and references such as the telephone number and the physical address that allow you to contact him are present on the site. Then you have to check that the online store allows other forms of payment in addition to the credit card, for example the sale on delivery. You can search for information about the seller using the search engines, in order to find reviews and methods of purchase on that website.

There are some tips and tricks to avoid being a victim...

- It would be useful to collect all the data to be sure of the real identity of the seller. The seller's data must be clearly indicated, i.e. the name of the company and the geographical address of the registered office.

- Before buying a product or using a service on the Internet, it is useful to check the sales policies and withdrawal conditions, delivery times, costs and shipping costs.

- What is important is the certification, that is, a certificate that proves the correspondence between a given site and a natural or legal person. In browsers there is a window called "security" which contains a special item "view certificates".

- It is always advisable to buy on sites with the precise indication of a quality mark, issued by an external body, which certifies that the site carries out activities in compliance with consumer rights.

- Care must be taken to purchase on a foreign site, since the reference regulations and controls to which they are bound may not be directly appreciable and lend themselves to criticism in cases of litigation.

- Do not use credit cards on the Net in an indiscriminate way, but pay if possible with prepaid cards trying to remain anonymous, unless the sites have a 128 bit SSL (Socket Secure Lock) data transmission protection system (currently the more advanced). To verify the presence of SSL, check that the drawing of a closed padlock appears on the lower part of the screen; if the transaction is not secure, the padlock will be open, or no padlock will appear.

- Verify that this is a fixed price sale. In the case of auctions, the guarantees for consumers are lower, it is therefore advisable to buy only on a site that publishes a clear regulation and that provides solutions in case of fraud by the seller.

- A very important thing is not to provide personal data if there are no guarantees for the processing of personal data.

- A useful and opportune thing to do would be to carefully keep a copy of all the orders made and the related documents (e-mails exchanged with the seller, information on the conditions of sale, etc.), as well as, in a particularly secure way, the passwords and codes, especially those for accessing financial Internet services.

- If you change your mind regarding the purchase made, you can exercise the right of withdrawal in the manner indicated on the contract by means of a registered letter with return receipt sent to the seller.

REGULATION AND SUPERVISION

Security, as we have seen, is primarily about money, could be physical or digital. The European Union intervened precisely on this through the establishment of a surveillance department and careful regulation regarding internet security, especially on electronic commerce.

It specified that the issue of electronic money poses regulatory and supervisory problems to which the European Union has not remained insensitive, given the lack of regulation on the matter. In fact, it must be understood that electronic money has characteristics that make it similar to cash. The operation of issuing electronic money is nothing more than a conversion of cash into a new form, that is, into the digital one. The issue of electronic money does not create money, but replaces it. So much so that features such as non-traceability can be maintained in the transition to the use of electronic money. It is a means of payment different from cash but similar to this.

To realize how we respond to the need for anonymity, we return to eCash technology, called the blind signature. In essence, it is not the bank that generates the electronic coins, but the software on the customer's computer that initiates this creation. It is the same program which then deals with the generation of random serial numbers. Then these coins are sent to the bank in a digital envelope. The message contained in the envelope, i.e. the coins with the relative random numbers, thanks to the random value, is not known by the bank. The latter merely affixes its digital signature through the envelope, thus ending the process of generating digital coins, of which, however, this time, it cannot know the serial number.

PROTOCOLS FOR SECURITY OF TRANSACTIONS

In a credit card payment, unlike what it might seem, the party who, in the abstract, runs the greatest risks from making a remote payment by credit card is the seller: in fact, by accepting the payment without checking the correspondence between the

credit card holder and the buyer, is in a legally very weak position. The buyer, on the other hand, will be able to validly benefit from a fairly strong protection: he or she will be able to bring an action of nullity of the contract against the seller and will also be able to claim that is not expressed the training intention of the contract; he or she may also obtain compensation from the issuing bank for the amount fraudulently paid. The bank, moreover, cannot validly raise a hypothetical responsibility of the holder for delay in the communication of loss, given and considered that an illegal use of his card can be made by third parties, even if the holder remains in the actual availability of the same. Failed purchases, fears about the security of transfers and dissatisfaction with the tools that can be used are obstacles with which to confront to ensure the development of internet commerce. Hence, the need to improve the security standard for transactions in order to build the necessary trust among network users. Fears about the security of transfers and dissatisfaction with the usable tools are obstacles with which to confront in order to guarantee the development of internet commerce. Hence the need to improve the security standard for transactions in order to build the necessary trust among network users.

SSL (Secure Sockets Layer)

An effective method to guarantee the security of online sellers is represented by the SSL (Secure Sockets Layer) protocol, which establishes a secure communication channel between a browser and an internet server. This protocol was implemented by Netscape Communications for use with Netscape Navigator. In the second half of the 1990s, Microsoft Corporation introduced a security technology for its new Internet Explorer browser called Private Communication Technology (PCT). The merger, then, between SSL and PCT, in order to provide a single proposal for a common standard for the internet, led to the creation of the Transport Layer Security (TLS) protocol. The fundamental component of a connection protected by SSL is represented by the SSL Handshake Protocol: it begins with a mandatory server authentication, while for the client it is optional; after the authentication process is concluded, the bargaining for the encrypted sequence takes place: the parameter thus decided will be used during the whole session and will guarantee the security of all data exchanges.

In an online payment, when a consumer (client) wants to buy something on the internet from a seller (server) using an SSL connection, there is a procedure that can be divided into two steps: at first, there is the constitution the session then exchanges information between client and server through a secure connection. At this point, the client can fill up his virtual shopping cart and then pay the bill. All the information that is thus output is still encrypted by the server with the SSL protocol; a request is sent to obtain a transit point with conversion of the protocols (gateway) for payment on the internet and, therefore, we will ask the bank for authorization. The SSL server then gets or authorization or refusal for the transaction through the payment gateway, and sends the result to the merchant and consumer. All this, however, does not ensure the protection of credit card data once they have been collected by the seller: if he or she does not guarantee the protection of the data received.

SET (Secure Electronic Transaction)

With the aim of improving the security of credit card payments, a specific protocol called SET (Secure Electronic Transaction) was developed in February 1996. This system guarantees: the confidentiality of the information processed; the integrity of

the messages; the certification of authenticity of the parties involved in the transaction. The SET credit card holder receives an encrypted certificate from the issuing bank under which he is uniquely identified by the credit institution. The cardholder registers the certificate on his computer and, when making a payment via the internet, gives the bank the possibility of certifying to the seller whether whoever is using the card is actually the card holder. In this way, the bank replaces the seller in the burden of verifying the correspondence between the signature of the person making the payment and the signature affixed to the back of the credit card, a charge which, obviously, in transactions via the internet, would be impossible to fulfill. In this way, the recipient of the payment is more guaranteed given that, in the event of problems, he or she will be able to protect himself against the buyer and against the issuing institution which, in practice, has not been able to guarantee a safe and inviolable system. The SET, to ensure the confidentiality of information, ensure the integrity of messages and authenticate the identity of users, uses cryptography with symmetric and asymmetric key.

HTTPS

The security protocols used on the network require equally secure application protocols such as HTTPS and SMTP and then conclude with TCP at the transport level. In particular, the HTTPS protocol is used to add security to the WWW pages in order to make applications such as electronic commerce possible. The combination of SSL with the normal HTTP standard allows obtaining a new protocol: HTTPS. This protocol ensures that personal information is sent in encrypted packages. In this way, the transmission of information takes place in a secure manner, preventing intrusions, tampering and falsification of messages by third parties. The HTTPS protocol therefore guarantees both the confidential transmission of data and their integrity. HTTPS is a URI (Uniform Resource Identifier) syntactically identical to the http://scheme but with the difference that the accesses are made on port 443 and that a level of encryption/authentication is interposed between the TCP and HTTP protocol. In practice, an encrypted communication channel is created between the client and the server through the exchange of certificates; once this channel has been established, the HTTP protocol is used for communication.

To set up a web server to accept https connections, the administrator must create a digital certificate or an electronic document that associates a person's identity with a public key. These certificates must be issued by a certificate authority or in any case by a system that verifies the validity of the same in order to define the true identity of the owner. In particular situations, such as in the case of companies with a private intranet, it is possible to have your own digital certificate which can be issued to its users. This technology can therefore also be used to allow limited access to a web server. The administrator often creates certificates for each user that are loaded into their browsers containing information such as their name and e-mail address so as to allow the server to recognize the user when the latter tries to reconnect without entering the credentials. Of course it goes without saying that this makes internet transactions much more secure.

CONCLUSION

We can affirm, after an analysis on what are the dangers on the internet and in particular in E-Commerce, that privacy and security walk together to guarantee the user, whether it is a buyer or a seller, the maximum possible protection. We have highlighted what the payment methods are and how they work, which are more secure and how they have evolved; we have seen the various disciplines on privacy and on the protection of one's personal data, guaranteed by specific bodies of the various States and by the European Union. All these factors combined together ensure that the E-Commerce market is in continuous development, not only, they do it ensuring maximum security and privacy for all users. At the same time, we were able to see how important customer support is for an E-Commerce; it is a fundamental element for the success of a shop and can guarantee an advantage over competitors. However, we have seen that it is important to set up efficient customer care to avoid customers being dissatisfied or, on the contrary, demanding too much.

All these factors, put together, are the basis of a successful E-Commerce store, so young entrepreneurs cannot disregard all of these. Moreover, they must be the first thing to manage before attempting such a type of business.

References

- Vademecum sul trattamento dei dati personali alla luce del GDPR
- E-Commerce: prospettive e dinamiche nel contesto italiano - Forner Leonard - Università degli studi di Padova - dipartimento di scienze economiche e aziendali ”M. Fanno”
- ALBERTO MAGNANI, Il Sole 24 Ore – Tech e digitale?
- CASALEGGIO ASSOCIATI, 2016. Focus sull’E-Commerce
- EUROPEAN COMMISSION, Bruxelles 1997. A European Initiative in Electronic Commerce

Sitography

- www.casaleggio.it
- ec.europa.eu/eurostat
- https://www.netstrategy.it/ecommerce/servizio-clienti-ecommerce-come-renderlo-il-punto-di-forza-del-tuo-negozio
- https://www.ninjamarketing.it/2017/04/12/limportanza-del-customer-service-per-il-tuo-ecommerce/
- Paypal http://www.paypal.com
- Gateway di pagamento Documentazione rilasciata dalla “Società Per I Servizi Bancari”
- http://www.carabinieri.it/cittadino/consigli/tematici/internet/i-rischi-dell'E-Commerce