

PROTEUS MANUAL

PREVENTION, INFORMATION AND SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT

PROTEUS



Co-funded by the Prevention of and
Fight against Crime Programme
of the European Union

APAV®
Associação Portuguesa de Apoio à Vítima
Apoyo à Vítima

[illegible]

ISBN Legal Deposit
978-972-8852-78-8

Telephone Fax
+351 21 358 79 00 +351 21 887 63 51

Title
Proteus Manual - Prevention, Information and
Support to Victims of Online Identity Theft

E-Mail Website
apav.sede@apav.pt www.apav.pt

Author
2015 © APAV
Associação Portuguesa de Apoio à Vítima

APAV
Rua José Estevão, 135 - A
1150-201 Lisboa
Portugal

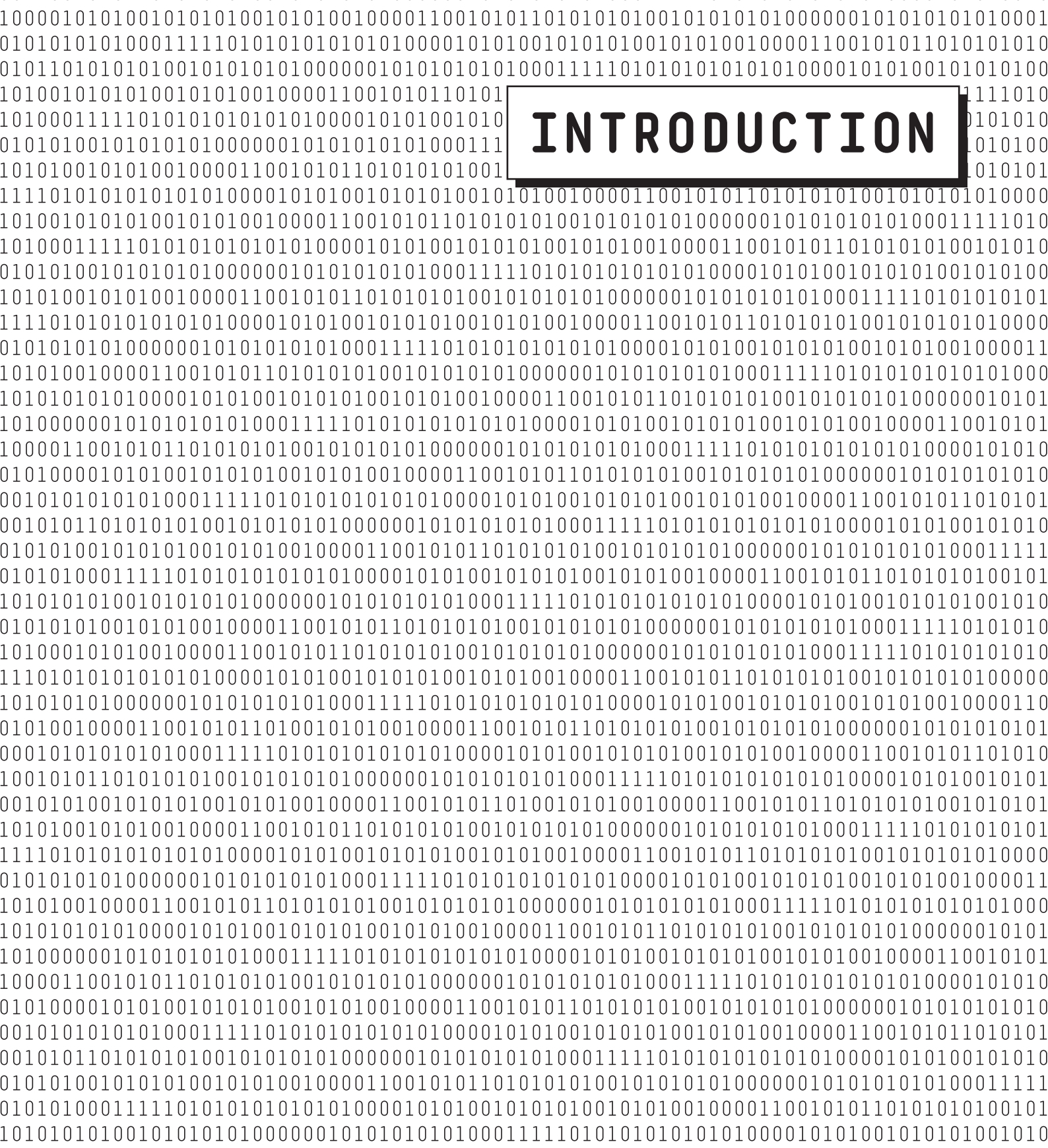
|||||

INDEX

|||||

INTRODUCTION	5	3.4.2. On society	35
1. STUDY CASES	9	3.5. Investigation difficulties	36
< Case 1 >	11	4. LEGAL FRAMEWORK	39
< Case 2 >	11	4.1. International scope	41
< Case 3 >	11	4.2. Portuguese law	42
< Case 4 >	12	4.3. Identity theft, domestic law and the	49
< Case 5 >	12	Convention on Cybercrime	
< Case 6 >	12	5. APPLICATION OF DOMESTIC LAW TO STUDY CASES	51
< Case 7 >	13	< Case 1 >	53
< Case 8 >	13	< Case 2 >	53
< Case 9 >	13	< Case 3 >	53
< Case 10 >	14	< Case 4 >	54
2. IDENTITY THEFT - FRAMEWORK	15	< Case 5 >	54
2.1. Cybercrime	17	< Case 6 >	54
2.1.1. Globalization	17	< Case 7 >	55
2.1.2. Definitions of cybercrime	17	< Case 8 >	55
2.2. Identity theft	19	< Case 9 >	55
2.2.1. Terminology difficulties	19	< Case 10 >	55
2.2.2. Definition attempt	20	6. PREVENTION	57
2.3. <i>Modi operandi</i>	21	6.1. Preventive measures	59
3. IDENTITY THEFT - THE REALITY IN PRACTICE	27	6.2. Signs of computer infection by malware	64
3.1. Most common situations of identity theft	29	6.3. How to identify signs of identity theft	65
through the Internet		7. CONTAINMENT	67
3.2. The perpetrator and the victim	30	7.1. Infection by malware	69
3.3. Risk factors	32	7.2. Identity theft	69
3.4. The impact of identity theft	33	ANNEX	73
3.4.1. On the victim	33	Glossary	75
a. FINANCIAL	33	Support service numbers of the bank institutions which	77
b. LEGAL	34	are members of the Portuguese Bank Association	
c. EMOTIONAL	34		
d. IMPACT ON DAILY LIFE	35		

|||||



INTRODUCTION

[illegible]

INTRODUCTION

A study which surveyed 13,022 adults aged between 18 and 64 years from 24 countries worldwide in 2013, estimates that there are 378 million victims a year, one million victims of cybercrime each day and 12 every second¹.

The percentage of online population victim of identity fraud committed through the Internet and of unauthorized access to their email in 21 countries worldwide varies between 1% and 17%, whilst the percentage of population from those countries victim of conventional theft and robbery varies between 1% and 5%².

Victims of cybercrime are in a particularly fragile and unprotected situation, as because of it being a recent phenomenon, it still is not well understood and it's misjudged by the population in general, being its effects underestimated also in what concerns the establishment and implementation of measures by the responsible entities to tackle it.

The cases of identity theft through the Internet may be very complex and victims may need personal assistance to help them recover from the situation. Many times help is needed to operate computer means to suppress cybercrime and victims may not know how to use them.

The impact of cybercrime and, specifically, of identity theft committed through the Internet, is increasing every day, as well as the number of victims filing complaints to the police and seeking help; thus there is the need to improve the response and the support to be offered.

In this scope, there was the need to draw up this guide, which, by focusing specifically on identity theft through the Internet, aims at preparing the staff of victim support offices to understand this phenomenon, in order to help crime victims to handle it the best way possible.

1 Norton Cybercrime Report, 2013.

2 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime - Draft, February 2013, p.3.

1.

STUDY CASES

[illegible]

1. STUDY CASES

< Case 1 >

Josué, bank employee, knew the access codes of the homebanking service of Joaquim and sold them to a criminal organization, which accessed the account and transferred 6000 euros to an unknown account.

< Case 2 >

Joana considers herself a briefed person on what concerns cybersecurity and takes cautions to protect her computer. One day, Joana, impressed by what she had read on a daily newspaper about the rise of cybercrime in Portugal, decided to do some research on the best antivirus available. In order to do so, she used a popular search engine and found, among many, a dubious page proposing the transfer of a potent antivirus, which she chose not to accept, since she had been warned to only accept the transfer of information from reliable sources. That night, Joana, undertook some payments she had to make using her bank's online page. A week later, Joana consulted the extract of her bank account and noticed the disappearance of a considerable amount of money.

< Case 3 >

Jandira and her kids use the Internet to do online researches and send e-mails. However, over the last month, Jandira's computer became so slow, that she and her children gave up using it. Last Monday, Jandira received an e-mail signed by ReidosHackers, which claimed to have her computer under its control and asked for a € 600 payment in order to return to her the free use of her own computer.

1. STUDY CASES

< Case 4 >

Josefina really likes exchanging e-mails with her friends and with family members, some of them immigrated in France.

One day, she was faced with an e-mail from her bank asking her to click on a link and subsequently confirm her details by filling in a form.

Josefina went to get her documents and did what was required of her immediately.

A month later, Josefina was contacted by her account manager who, intrigued by the transfer of much of the money saved to an unknown account, decided to clarify his doubts with the client.

< Case 5 >

José received an e-mail, which was part of a spamming scheme, which apparently was sent by his webmail service, asking him to update his password.

Afterwards he was questioned by some of his workmates and friends, about some e-mail messages that they had been receiving from his e-mail address, where he was asking them for financial help. None of his friends responded to these e-mails.

< Case 6 >

Joel and Jessica dated for 5 months and then Jessica broke up. Joel, enraged, swore revenge and Jessica ignored him.

One day, when she arrived to the school in the morning, she noticed that all her classmates looked at her, whispering to each other and laughing. After entering the classroom she asked her colleague Jurema if she knew the reason for so many laughs and she told her that there was a profile in the social network Facebook, in Jessica's name and with her profile photo, where she was proclaiming to have sexual intercourse in exchange for small sums of money.

1. STUDY CASES

< Case 7 >

Joana, which knew the complete name and address of Juliana, created an e-mail with her name and signed in to an online auctions site with Juliana's name, address and using the e-mail with her name. Afterwards Joana published adverts for the sailing of tablets. João, interested in acquiring one, paid for one but never got the equipment. Sometime later, the mailman knocked on Juliana's door and handed over a summons for her to be interviewed two days later as a suspect of committing a fraud offence.

< Case 8 >

Julieta received a phone call from someone who claimed to be from "Novo Banco" and that she needed to confirm some of her personal data. Julieta accepted, relieved to hear that she had not stood linked to "Banco Mau".

Two months later, Julieta received an account related to some online purchases made with her credit card information.

< Case 9 >

Several messages appearing to be sent by the clients' webmail service and asking for an update of the account password were sent to many e-mail addresses. Júlio's wife entered her data and so the criminal had access to her inbox, getting to know many of her and her family personal information.

Júlio was then contacted by two credit institutions who wanted to confirm if the credit applications on his behalf were legitimate. Júlio, who had never resorted to credit, explained he did not make any application with any of those institutions. He was astonished by the amount of personal data that the fraudster knew about him! The applications were refused.

A month later, Júlio went to his bank in order to ask for a loan to buy a house. The loan was refused due to there being many applications for credit made on his behalf in the past months.

1. STUDY CASES

< Case 10 >

Jair has been a victim of bullying since he entered Odivelas High school.

One day, Jair came home and logged into his profile on the social network Facebook. His heart stopped beating for a moment when he found out that several pictures of him in underwear had been published using his account.

Despair took over when he remembered that the only person who knew his Facebook username and password was Jaime, his only friend.

2.

IDENTITY THEFT - FRAMEWORK

[illegible]

2. IDENTITY THEFT – FRAMEWORK

2.1. Cybercrime

2.1.1. Globalization

In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the Internet³. By the year 2020, it is estimated that the number of networked devices will outnumber people by six to one. Thus, crime will more and more “make use” of the Internet.

Information and Communication Technologies (ICT) are new means to commit offences. Global connection through the Internet and the use of such technologies also enable new legal elements of crime to emerge.

ICT also facilitate crime internationalization, i.e., for instance, the perpetrator can easily commit an offence in Brazil against a victim in Portugal, what usually happens in cases of “phishing”, as described in Case 4 of this guide.

Cybercrime has thus been increasing, being committed both by criminal organizations and by individual criminals seeking new opportunities for obtaining profits and other advantages or in view of intimacy matters, notably through social networks.

2.1.2. Definitions of cybercrime

There is no consensual and universal definition of cybercrime. National and international laws do not define the term and there is no consolidated doctrine on this matter.

According to the United Nations Office on Drugs and Crime, definitions of cybercrime depend upon the purpose of using the term.

The said Office, given that national and international instruments do not give a per se definition of cybercrime, tries to describe the contents of the term by enumerating the conducts or acts it comprises⁴. Thus, this Office presents a non-exclusive list of fourteen behaviors likely to be considered as cybercrime, classified in three categories:

3 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime – Draft, February 2013, p. 1.

4 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime – Draft, February 2013, pp. 11 e 12.

2. IDENTITY THEFT – FRAMEWORK

Acts against the confidentiality, integrity and availability of computer data or systems	Computer-related acts for personal or financial gain	Computer content-related acts
> Illegal access to a computer system; > Illegal access, interception or acquisition of computer data; > Illegal data interference or system interference; > Production, distribution or possession of computer misuse tools; > Breach of privacy or data protection measures.	> Computer-related fraud or forgery; > Computer-related identity offences; > Computer-related copyright and trademark offences; > Sending or controlling sending of spam; > Computer-related acts causing personal harm; > Computer-related solicitation or grooming of children.	> Computer-related acts involving hate speech; > Computer-related production, distribution or possession of child pornography; > Computer-related acts in support of terrorism offences.

In its communication to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime – the European Commission defines cybercrime as “criminal acts committed using electronic communications networks and information systems or against such networks and systems”.

It seems to us that the division of the concept of cybercrime into an extensive concept and a restrict concept is thorough and clear⁵, comprising the former all criminal acts committed resorting to computer means, even if such means are merely used as tools for committing them and are not an element of an offence; and the later comprising only the offences where the digital component is an element of an offence or even its object.

5 Please see Dias Venâncio, Pedro, *Cybercrime Act - Annotated and commented*, Coimbra Editora, 2011, p.17.



2. IDENTITY THEFT – FRAMEWORK



2.2. Identity theft

2.2.1. Terminology difficulties

There is a lot of dispute around the term “identity”, that’s why first of all we shall mention that within the scope of this guide, this term shall mean all data concerning a person, the use of which by a third person allows this third person to commit criminal acts pretending to be the former one.

The term “furto de identidade - identity theft”, although chosen to be used in this guide, does not define accurately the phenomenon it intends to address.

In fact, none of the terms usually used in this context, due to the influence of the terms used in the English language – “furto de identidade – identity theft”, “roubo de identidade – identity robbery”, “fraude de identidade - identity fraud” – is terminologically accurate.

In fact, the cases we will address assume that the criminal obtains personal data or certain passwords or personal codes of the victim and uses them to commit offences.

We cannot say it is theft or robbery as according to the Portuguese Penal Code – sections 203 and 210 – stealing personal property does not include obtaining data or passwords.

We also cannot say it is “fraude - fraud”, as this term is not acknowledged by Portuguese law.

As regards the English language, the terms “identity theft” and “identity fraud” seem to be used, in most cases, with the same meaning, being “identity theft” mostly used in the United States of America and “identity fraud” in the United Kingdom. In the United Kingdom nevertheless there was an attempt to delimit the meaning of each one of these terms⁶.

In this guide, we chose to use the term “furto de identidade” [“identity theft”] to name the phenomenon addressed, as it seems to us that using the term “fraude de identidade” [“identity fraud”], due to lack of legal content, and the term “roubo de identidade” [“identity robbery”], due to lack of violence or coercion as regards the conducts this phenomenon comprises, is no option.

Thus, “identity theft” although not being an accurate designation, seems to be the one corresponding most to the behaviours which we intend to define and study.

6 Identity theft or “furto de identidade” [in Portuguese] is to obtain a person’s identification data without his/her knowledge or permission, and identity fraud or “fraude de identidade” [in Portuguese] is to use someone else’s identity for criminal activities, in order to obtain goods or services by deception; cf. James Jones, *Understanding ID fraud and how to stop it, The Anonymous Attacker*, CIFAS, 2009, p.6. Both meanings are comprised in the notion of identity theft through the Internet used in this guide.



2. IDENTITY THEFT – FRAMEWORK

2.2.2. Definition attempt

As for cybercrime, there is no common definition of identity theft. We will try to define which acts we consider as being comprised in this phenomenon, for the purposes of this guide.

First of all, we must mention that in Portugal identity theft is not an offence, but rather a phenomenon to which several legal elements of crime apply.

According to the US Federal Trade Commission, “Identity theft occurs when someone uses personal information of another person, without their knowledge or consent to commit fraud or other offences”.

Pursuant to the European Commission Fraud Prevention Expert Group, the core of the phenomenon, resulting from the definitions given for identity theft and identity fraud, is the appropriation and use of someone’s identification data to commit illegal activities.

According to the Council of Europe Economic Crime Division, the term “identity theft” describes the acts where the perpetrator obtains and deceitfully uses another person’s identity. These acts may be committed without the help of technical means, but can also resort to computer technology.

Some definitions, which vary from country to country, focus more on the act of obtaining data, while others require the intent of committing certain illicit acts after obtaining such data.

The common denominator to the several definitions proposed is that the described conduct concerns one or more of three phases – the phase of obtaining personal data, the phase of possessing or transferring data (knowing that data will be used to commit a crime) and, finally, the phase of using data to commit crime.

Attempting to give the widest definition possible, we can say that identity theft comprehends obtaining without consent the victim’s personal and/or secret data, possessing or transferring them being aware that they will be used for criminal purposes, and using them to commit offences.

As this guide deals with identity theft through the Internet, the acts will be comprised in the definition of the phenomenon, regardless of the victim’s personal data being obtained through the Internet (as in cases 2, 4, 5 and 9) or obtained by another means but then transferred through the Internet or used to commit an offence through the Internet (as in cases 1, 7, 8 and 10). If the

7 This definition is used in the guide to assist victims of crime of the Office for Victims of Crime at the US Justice Department.

2. IDENTITY THEFT – FRAMEWORK

offence concerns only one of the phases, the corresponding conduct – obtaining, possessing or using – has to be committed through the Internet in order to be included in this concept.

As already mentioned, after obtaining the victim's data the criminal can use them to commit offences. Those offences will be of three types: offences not directly linked to the victim but committed with the victim's name (as in cases 5 and 7), offences aiming at the perpetrator's or a third party's enrichment and that directly harm the victim (as in cases 1, 2, 4, 8 and 9) and offences aiming at slandering the victim (as in cases 6 and 10).

2.3. *Modi operandi*

Obtaining the victim's data may be achieved by various means, which tend to multiply and diversify. In this scope, there is constant innovation aiming at “outwitting” the users' detection mechanisms and authority actions. For this reason, we have to address the various means in a general way, so that it won't be quickly outdated.

There are traditional methods for obtaining someone's personal details, such as ransacking the garbage, intercepting mail, stealing certain identity documents or other documents or reports containing personal or financial information about the victim, pretending to be a landlord, a potential employer or another person that could ask for this kind of documents, trying to obtain information from persons close to the victim, contacting the victim or the banks on false pretexts to obtain insider information (as in case 8), buying such information or observing the victims while they are using the information they want to obtain (as in the case of the victim's coworker who observes her entering the account access data, in order to use such data later to withdraw money from the account).

All these means may be comprised in the concept of identity theft through the Internet, according to our definition, as information gathered by non-computer means may be used to commit an offence through the Internet.

Another method – material but not traditional – for obtaining the victim's data is the theft of hardware or of a mobile phone containing personal or secret information about the victim.

After addressing the main traditional methods, we shall address the methods resorting to new

2. IDENTITY THEFT – FRAMEWORK

technologies, more precisely, to the Internet.

The so-called “Nigerian Letters” – that initially emerged as letters, telex and telefax messages and currently consist in electronic mail messages – are a means to commit identity fraud, both resorting to traditional means of obtaining data and to the Internet.

Such correspondence is usually written in “bad” English; traditionally such letters were addressed to persons in important positions within the corporate environment, public administration, politics and other influential sectors of society, but nowadays they are sent in a widespread way. The sender identifies himself as being part of the government senior staff or of a state-owned company from a certain African country, or as a relative of such a person.

During the first years the issuing country was predominantly Nigeria. Then, it spread to some countries geographically close to Nigeria and recently this type of correspondence also comes from South Africa.

The message consists in a business proposal. The sender states having a huge amount of money obtained from his privileged status linked to his country’s administration.

The sender justifies the need to transfer such money abroad by saying he cannot be publicly associated with such wealth, due to its origin. Thus, he asks the recipient to receive such amount in a bank account he is the holder of, receiving a consideration of 20 percent, or even 35 percent, of the amount. For that purpose, the sender asks the recipient to send his account’s data, personal details, details of his company or organization, including headed paper, etc.

These data are not always requested in the first letter or email message, but rather in following ones, after a reply from the recipient, thus enabling to establish a dialogue.

Holding data of natural persons, corporate bodies and of bank account, fraudsters can commit frauds at international level (which occasionally happens), by fraudulently using such information within the financial system.

Job advertisements published in newspapers, on the Internet, etc. may be false and aim at gaining the victims’ attention to obtain their data to commit fraud and identity theft. These are the so called job scams, which resort to traditional means to obtain data as well as to the Internet.

2. IDENTITY THEFT – FRAMEWORK

At this point it is also important to mention help requests sent through the email address or the Facebook account of someone known. Phishing for gaining access to someone's electronic mail is many times used to confer credibility to these help requests – as in case 5. Identity theft victims' Facebook account is acceded with the same purpose and help requests may be posted on the profile page, reaching all the victim's friends or be sent through private messages.

Facebook may also be used to obtain data of new identity theft victims. By infecting computers with malware, links to pages requiring certain data from new victims are posted on the victims' Facebook pages. A video is published, for instance, on a victim's page and his/her friends are forwarded to a page requesting them to enter their personal data to “like” the video.

Search engines, like Google, which allow searching millions of pages in a few seconds, may be used for unlawful purposes.

The term Googlehacking is used to describe complex searches in these search engines, aiming at finding unprotected targets and sensitive data in websites. The Google Hacking Database facilitates this task. It's a new database for searches identifying sensitive data. The Google Hacking Database detects server alerts and vulnerabilities, error messages that contain too much information, password files, sensitive directories, pages containing login portals, pages containing network or vulnerability data such as firewall logs, and although Google's efforts to block hackers' attempts, nothing stops them from infiltrating the websites and viewing Google Hacking Database.

Many times, company workers and employees (or someone pretending to be them), having access to identity and secret information of the company where they work, of the management and administration members, of other employees or of the company's clients, obtain their data with criminal intent; many times aiming at selling the information, predominantly to criminal organizations. This is what happened in study case 1.

One of the most commonly used methods for obtaining personal details for identity theft and to which authorities and the media have been paying much attention is the so called “phishing”.

This action translates in the mass sending of electronic mail messages (spamming), with a link to a page on the WWW. Usually this page is an approximate reproduction of a bank or credit institution page, for instance, and contains identifying elements and images of the legitimate entity. Nevertheless, it's a fake page. If victims use the link to have access to the fake page, they

2. IDENTITY THEFT – FRAMEWORK

will be asked to identify themselves and to enter the confidential codes of their bank account or card. These data will allow the person who created the page to have access to the victims' bank accounts and to transfer the money they have there or to use their credit card.⁸ Case 4 aims at depicting a classic example of this phenomenon.

We may identify four phases in phishing: the initial phase consists in a massive sending of electronic mail messages containing a link to a webpage; in the second phase, victims give the perpetrator their personal information/password/access codes – most times this moment will consist in entering the victims' personal details into the fake website; in the third stage, the perpetrator accedes to the legitimate webpage of the bank institution, enters the victims' data and withdraws money from the account; and the fourth stage consists in money laundering (a process by means of which some perpetrators of some criminal activities conceal the origin of goods and proceeds (advantages) unlawfully obtained, transforming the liquidity from such activities in legally reusable funds, by disguising the origin or the real owner of the funds).

When addressing the new methods for obtaining private data to commit identity theft, we shall also underline “pharming”, a “technique that uses methods for disseminating viruses in form of worm – the worms. It consists in disseminating concealed files through spam – i.e. electronic mail –, which also in a concealed way auto-install themselves on victims' computers or computer systems. Without the computer owner being aware, after being hosted, these files change in a covert manner the system archives, namely the files containing the popular “favorites” and the cookies record. With this change, when the computer owner accedes to his usual bank website, the cunningly changed system redirects him/her to another website, created and available online using methods similar to the ones used for phishing.”⁹

In this scope, another technique we must mention is sniffing. Networking computers share communication channels. In shared channels computers may receive information sent to other computers. Capturing information sent to other computers is called sniffing.

At last, we must mention hacking and cracking, both being ways to illegally accede to computer systems, being thus also means to gather private information. In this context, both terms mean the act of breaching security codes or illegally obtaining program license codes, without consent, to gain access to another person's computer. Case 3 describes a situation of infection by viruses of Jandira's computer, reason why it was running so slow. Many times hackers infect victims' computers to subsequently require a ransom, i.e., an amount of money to solve the

8 Cf. Pedro Verdelho, Phishing and other ways of defrauding on communication networks, Information Society Law, Vol. VIII, p. 417.

9 Pedro Verdelho, Phishing and other ways of defrauding on communication networks, Information Society Law, Vol. VIII, pp. 415 and 416.

2. IDENTITY THEFT – FRAMEWORK

problem they caused. This is not a case of identity theft through the Internet, unless the hacker has obtained Jandira's data by acceding to her computer.

Data mining consists in analyzing data, attempting to create patterns and establishing relations between them. This technique is used in many search areas. There are computer programs, the so-called "data miners", that collect information available on the Internet or from the victims' computers, without consent, analyze such information and generate patterns. This enables companies, for instance, to foresee consumers' behavior; as regards identity theft, these programs allow to organize the victim's identifying data so that the cybercriminal can use such data.

We shall finally focus on keylogging, which consists in using a computer program that, after being installed on the computer, allows recording everything typed with the keyboard. This method deceives even the most careful internauts, as Joana, the victim in case 2. The victim only had to open the page offering to transfer the antivirus, to have software installed on her computer, allowing Joana's bank account access data, subsequently entered into her bank's website using the keyboard, to be recorded in the computer of the criminal who afterwards used them to gain access to Joana's account and withdraw money.

3.

IDENTITY THEFT - THE REALITY IN PRACTICE

[illegible]

3. IDENTITY THEFT - THE REALITY IN PRACTICE

3.1. Most common situations of identity theft through the Internet

The main realities addressed in this guide, chosen for being the most common ones, shall be phishing for gaining access both to another person's email account (as in cases 5 and 9) and to another person's bank account (as in case 4), and slander on social networks (as in cases 6 and 10).

First we shall address phishing for gaining access to the email account. After obtaining the victim's confidential and personal data through any of the more sophisticated methods in the previous chapter, the computer criminal may gain access to the victim's email account aiming at learning the content of the mailbox, at establishing contact with the victim's bank – usually with the account manager – or at using such email account to give credibility to electronic mail messages he intends to send and which usually are requests for financial help and ways of obtaining personal details of other potential victims.

Thus, the two main purposes of phishing for gaining access to the email account are gathering confidential and personal data of the victim (by viewing the victim's mailbox or contacting the bank) to commit bank fraud, or to simply deceive the friends or acquaintances of the identity theft victim to cause them to transfer money to the credit of the criminal or to cause them to give him their personal data. Thus, we can see that many times phishing for gaining access to the victim's email account may have as ultimate goal gaining access to the victim's bank account and subsequent bank fraud.

Unfortunately, “study” phishing for gaining access to the victim's bank account, as described above, is already very common in our country.

In a different perspective, there is identity theft for slander in social networks. This kind of situation often occurs in the scope of friendship or dating relationships, in particular among teenagers and young people.

So, there are two forms of identity theft for slander on social networks: setting up a fake page or profile with the victim's data and in the victim's name, offending the victim's honor and individual consideration by resorting to pictures or phrases (as in Case 6), and using the victim's real profile to disseminate also offensive facts, judgments and pictures (as in Case 10).

3. IDENTITY THEFT - THE REALITY IN PRACTICE

In these cases, it is usually the victim who in the context of a close relationship gives data to the criminal allowing him/her to gain access to the victim's personal page on a social network or to the facts and images used to humiliate him/her.

3.2. The perpetrator and the victim

In this scope, we must distinguish the profile of a criminal committing identity theft with lucrative intentions from the profile of a criminal committing identity theft for slander on social networks.

Attempting to trace the profile of the perpetrator of identity theft in the former type of identity theft, it is worth to distinguish between the perpetrator who knows the victims due to being their friend, a relative or having any legitimate relationship with them (works in the victims' house, is their accountant, lawyer, etc) and, for that reason, it is easier for him to gain access to their personal information, choosing the victims for that reason, and the unknown perpetrator, who looks for victims at random. In these cases, it is very difficult to identify the perpetrator, as many times besides committing the criminal acts at the opposite side of the globe, in relation to where the victim is, the perpetrator always uses the victim's identity, so that his own personal data are not disseminated. For this reason, not many perpetrators of these offences and their characteristics are known.

At the beginning, the cybercriminal was considered to be an introverted computer expert male student, having an over average IQ and limitations as regards social interaction, being driven by the challenge of defeating the machine and by the desire to prove his intellectual superiority in view of society.

However, reality evolved. Nowadays the perpetrator of identity theft committed through the Internet can be anyone and his/her motivation is to get the victims' information needed to obtain gains and benefits.

Considering the wide range and variety of means available to get data of potential victims – which may require specialized skills or simply ransacking the garbage bin – the perpetrator of identity theft can be a highly or poorly qualified person, belong to any social class and have the most diverse personal characteristics.

3. IDENTITY THEFT - THE REALITY IN PRACTICE

The number of pages on the WWW showing how to commit computer offences renders it increasingly easier for a common person in need of money to commit a scam as the ones mentioned.

A type of perpetrator we must highlight in this scope is the so called insider. An insider is a highly qualified employee, in whom his employer trusts and who takes advantage of his knowledge about the company and the operation of the computer system, to obtain, sell or use insider information to commit offences.

Most dangerous instigators of this type of offences are criminal organizations that control the whole process of identity theft, from data gathering to money laundering¹⁰.

As regards the victim, we must stress the fact that the victim may also be any person. The most decisive factor for a criminal to choose a victim is the ease in obtaining the victim's personal details needed to commit the intended offence. This doesn't necessarily mean that the perpetrator is someone close to the victim, having access to the victim's mail, documents or computer, such as a relative, a friend or another person having a legitimate relationship with the victim, although it often is the case.

Nevertheless, according to statistics in the United Kingdom the most common target of these criminals is a male, between 40 and 50 years of age and having a job¹¹. Criminals seek victims who have money, either because they want to steal that money, or because they want the acts they commit in the name of the victim to be credible, namely when attempting to obtain credit.

In the United States of America, there is a higher incidence of identity theft among households with annual income over 75,000 dollars and among the population aged between 16 and 34 years¹².

Many times, victims are companies, banks, insurance companies or financial entities that prefer not to report the situation, solving the problem at internal level, assuming the losses for fear that public knowledge of the situation might lead to their discredit.

In the scope of social networks, identity theft is committed by persons closely linked to the victims, who for some reason decide to harm them by creating a fake profile with the victims' identity, for instance, or by using their real profile and slander them. This often happens among ex-lovers seeking revenge.

10 In this scope we can distinguish three types of operatives: the ones who gather the victim's personal information needed; the ones who find a way to use the stolen identity by falsifying documents, for instance; and the ones who use another person's identity to commit offences. The task division within such organizations aims at keeping perpetrators separate, thus maintaining the several parts of the organization anonymous to protect the "whole" of the organization, in case one part will be discovered by police authorities.

11 Sandra Peaston, The anonymous attacker and the not so anonymous victim, The Anonymous Attacker, CIFAS, 2009, p.20.

12 Cf. Lynn Langton and Michael Planty, Victims of Identity Theft, 2008, Bureau of Justice Statistics Special Report, 2010, p. 3.

3. IDENTITY THEFT - THE REALITY IN PRACTICE

3.3. Risk factors

As victims may be any person, it will be very important to know in which circumstances Internet users are more vulnerable and the risk of victimization increases.

Personal details on common persons are more and more available to the public, namely through the social networks, and computer criminals take advantage of it.

There are some conducts that increase the risk of using social networks, namely:

- › Not activating privacy options or having an easily accessible profile;
- › To make available or share too much information;
- › To accept friendship requests from unknown persons;
- › To post intimate pictures on social networks.

Working several hours online increases the risk of being a cybercrime target, in particular if working from home and using the personal computer, as unlike employees of companies having computer experts for protecting their computers, freelancers' computers have usually a lower protection against computer attacks.

There is a myriad of behaviors increasing the risk of becoming a cybercrime victim, namely:

- › Not having an antivirus or anti-spyware computer program installed;
- › Clicking on unknown links;
- › Viewing contents for adults;
- › Replying to messages on social networks, to emails or to any contact by any other means sent by unknown persons;
- › Carrying the password or Pincodes in the wallet, or keeping these in an unprotected file;
- › Disclosing, even to trusted persons, passwords or Pincodes;
- › Using easily accessible information to set up passwords, such as the date of birth, the mother's name or the pet's name;
- › Keeping important documents in unsafe places;
- › Disposing of documents without destroying them;
- › Sending confidential information via email;
- › Not updating antivirus software and other software installed in the computer;

3. IDENTITY THEFT - THE REALITY IN PRACTICE

- › Using free Wi-Fi connections.

3.4. The impact of identity theft

3.4.1. On the victim

Although victims may be anyone, certain groups with lower income, minorities and elderly people will suffer a stronger emotional, physical and financial impact, as they may have more difficulties in filing a complaint, filling in forms, reading documents and contacting victim support offices. Many times they have low economic resources, may face linguistic obstacles, may fear suffering retaliations if reporting the crime and may not recover from losses if they don't have access to credit.

a. FINANCIAL

Economic impact may be of two kinds: direct economic loss, i.e. the amount of money the perpetrator obtained by using the victim's identity, including the value of goods, of services or the monetary value obtained; and the indirect economic loss, which includes all costs the victim has due to identity theft (costs of legal actions, phone calls, mail, etc). Approximately 62% of victims of identity theft state to have suffered one of these economic losses, according to a survey concerning the years 2006 and 2007¹³.

In 2011, the total financial costs for victims of identity theft was approximately 17.3 billion dollars for the time period 2006 and 2007¹⁴ in the USA and 388 billion dollars in 24 countries worldwide¹⁵.

In cases of identity theft for committing bank fraud or fraud related with credit cards, institutions may have to refund victims for their losses.

In Portugal, according to the case law of higher courts, section 796 of the Civil Code – risk liability in contractual matters – or section 799 of the Civil Code – presumption of guilt – have been being applied to cases of identity theft to commit bank fraud. Thus, the bank institution will have to prove that it was not their fault or that it was the victim's fault, for not having to compensate the victim for the damage suffered.

13 Cf. LYNN LANGTON AND MICHAEL PLANTY, Victims of Identity Theft, 2008, Bureau of Justice Statistics Special Report, 2010, p. 4.

14 Cf. LYNN LANGTON AND MICHAEL PLANTY, Victims of Identity Theft, 2008, Bureau of Justice Statistics Special Report, 2010, p. 4.

15 Norton Cybercrime Report, 2011

3. IDENTITY THEFT - THE REALITY IN PRACTICE

Victims may lose their home and have their savings wiped out. Victims of fraud to use their credit account may struggle to get new credits or loans and to borrow on mortgage.

b. LEGAL

Victims may be considered suspects or defendants and be charged with offences they did not commit (as in case 7).

Victims may face civil liability proceedings for facts they did not commit or for contractual liability for obligations they did not enter into.

c. EMOTIONAL

Although the psychological impact differs from person to person, depending on victims' characteristics, some of the most common symptoms are fear, anxiety, anger or even a constant and time-extended distrust about everything and everyone that many victims describe as "paranoia". Emotional impact from identity theft is described as being similar to the victims' reactions to violent crime. Many victims feel their privacy was violated, feel helpless, powerless and fear that it will happen again.

Victims may be reluctant to report the offence to police authorities if they find out that the perpetrator is a person close to them they trusted in, such as a relative or a friend. Victims may also feel ashamed for having been cheated on.

Insecurity generated by loss of financial stability has a very strong impact on these victims. Furthermore, they might need to prove their innocence.

Many victims blame themselves for what happened and wonder who to trust in and if justice will be served.

Victims of identity theft through the Internet and of cybercrime in general may feel being treated as "second-class" victims, having less support than the remaining victims, as these offences are socially still undervalued and there are not many offices helping victims

3. IDENTITY THEFT - THE REALITY IN PRACTICE

restore their lives. These victims often also will have to deal with the disappointment of not being possible to identify the identity “thief”.

We must bear in mind that as these victims learn of new debts or other crime consequences, they are constantly revictimized.

The impact of crime is different when the perpetrator is a person close to the victim. In this case, the victim may feel pressed to assume liability for the offence to protect the criminal against the corresponding consequences.

d. IMPACT ON DAILY LIFE

For the victim, identity theft implies a serious trouble and loss of time when the victim tries to remedy its consequences. In the USA it is estimated that victims spend on average 97 hours for amending damage caused by such an offence, spending on average 1,884 dollars with it (data from the American organization Identity Theft Resource Center). On the other hand, estimates for the United Kingdom suggest that a victim spends between 3 and 48 hours “cleaning his/her name”¹⁶.

40% of victims state that loss of time was the worst consequence of crime¹⁷.

3.4.2. On society

In the United Kingdom, the cost of identity theft to the country’s economy was calculated at 1.3 billion British Pound every year. Estimates of annual losses in Australia vary between one billion and over 3 billion Dollar. In 2005, losses in the United States were estimated at 56.5 billion Dollar¹⁸. In the district of Lisbon, phishing resulted in damages of over 2 million Euro in 2011¹⁹.

Identity theft has an increasing cost for institutions such as banks, insurance companies, suppliers of goods and service providers. These institutions cover the financial losses suffered by victims, unless proved that the victim was negligent. This impact on institutions should not be disregarded, also because it will end up having an impact on the costs consumers will have to support to use the company’s services.

16 Fraud prevention expert group, Report on identity theft/fraud, Brussels, 2007, p. 10.

17 Norton Cybercrime Report, 2011.

18 Marco Gercke, Internet-related identity theft, Economic Crime Division, Directorate general of Human and Legal Affairs, Strasbourg, France, Council of Europe, 2007, p. 5 and 6.

19 <http://www.asjp.pt/2012/04/03/judiciaria-crisis-unidade-especial-para-investigacao-cibercrime/>

3. IDENTITY THEFT - THE REALITY IN PRACTICE

Companies can also have their identities used without consent; in such cases, they will have indirect losses with the investigation into their employees, with investing in preventive measures and in insurance.

The discredit that may affect those companies should also not be underestimated due to its impact on the economic system.

States and their governments may suffer direct losses, as in many cases identity theft is committed against public bodies, but they suffer mainly indirect losses, as they will have to invest funds in preventive measures and training, as well as in resources for police and judicial authorities.

3.5. Investigation difficulties

Identity theft through the Internet and cybercrime in general poses serious problems to police and judicial authorities in matters of investigation. Crime characteristics as well as other crime-related factors render it very difficult, sometimes almost impossible, to identify the perpetrator and to establish the circumstances of the offence.

Identity theft has a cross-border, international dimension, like cybercrime in general and the Internet. If the perpetrator and the victim are not in the same country, investigation is harder, as, besides the need to follow a potentially worldwide cybernetic trail, it requires cooperation among police and judicial authorities from all countries involved. According to the principle of sovereignty one country is not allowed to carry out investigations in another country without the consent of local authorities. Cooperation between the authorities of the several countries implies observing formalities and is time consuming, impairing investigations.

Cybercrime is said to be atemporal, as there may be an undefined time span between perpetrators committing the initial action it being materialized in a result, which, again, does not render investigations easier.

Many of the procedures to commit cybercrime may be programmed to happen automatically recurrent (spamming, for instance), providing such crime with a permanent nature.

Criminals use technologies enabling them to remain anonymous, as spoofing and other anonymity and coding programs.

3. IDENTITY THEFT - THE REALITY IN PRACTICE

The high level of technicity a cybercrime investigation requires implies the engagement of several entities with specific knowledge and the use of many internal, logistic and human resources, which are limited.

Besides these specificities, there are other factors impairing the investigation.

Cybercrime victims not filing a complaint are estimated at 80%.²⁰ This results from lack of awareness of their status as a victim and of information on how to file a complaint, as well as from lack of belief in the criminal investigation system and from the sense of impunity they have towards these offences. Another reason for victims not filing complaints is the shame they feel for having been cheated on.

Businesses, banks, insurance companies and financial entities choose to deal with the problem at internal level, absorbing losses, and not filing a complaint with the authorities, fearing that if the public learns of the computer attack they might be discredited and lose the trust from the market and clients.

The number of victims increases every day, according with the increase in the number of Internet users.

There are online pages containing information on how to commit certain computer offences and it is easy to find them through searches on well-known search engines.

Every day criminals also draft new ways to gain access to personal details and to commit offences using them. New technologies are swiftly disseminated through the online black market.

A huge hindrance to cybercrime investigation is the serious difficulty in having access to electronic evidence. In order to establish the origin of the communication, i.e., the IP address (Internet Protocol Address), it is necessary to have access to the record of historic files stored by Internet service providers, whose cooperation is crucial.

It is also relevant to secure the viability of digital evidence. Thus, the access, collection, preservation and analysis shall always be carried out according to specific procedures, a task to be carried out by specialists. Evidence collection must be done as soon as possible, as it can be very easily destroyed. For this to be possible, it is crucial to have the cooperation of Internet service providers, which are liable to preserve certain data only for a limited period of time.

20 United Nations
Office on Drugs and Crime,
Comprehensive Study on
Cybercrime - Draft,
February 2013, p. 117.

4.

LEGAL FRAMEWORK

[illegible]

4. LEGAL FRAMEWORK

Implementation of proper legislation plays a fundamental role in the prevention and fight against cybercrime.

Legislation is very relevant in the scope of criminalizing conducts, police authorities remit and powers to investigate, electronic evidence collection and preservation, jurisdiction, cooperation and information exchange, among the several national entities and the international entities, as well as in the scope of the liability of Internet service providers.

Although at national level States are most focused on criminalizing conducts, the need to develop legislation concerning the other matters has also been acknowledged.

4.1. International scope

In recent years much attention has been paid at international level to tackle cybercrime. We must highlight the actions developed by the Council of Europe, the European Union and the United Nations Organization on this matter.

The Council of Europe Convention on Cybercrime, of 23 November 2001, is the most used international instrument for implementing domestic laws on cybercrime.

Considering the informatization of the World and the risk that new technologies and the Internet may be used to commit crime, the Council of Europe Convention on Cybercrime aims at pursuing a common criminal policy to protect society against cybercrime based on international cooperation and the harmonization of domestic legislation. Below we will address the offences established by this international instrument and their application in the several phases of identity theft through the Internet, according to our definition.

Within the European Union we must highlight Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU of the European Parliament and the Council, replacing the Framework Decision.

Framework Decision 2005/222/JHA aimed at improving cooperation among member States' police and judicial authorities and standardizing penal rules on cybercrime.

4. LEGAL FRAMEWORK

Directive 2013/40/EU of the European Parliament and the Council replaced the Framework Decision, as mentioned, being its main goal “to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities (...)» It establishes the criminal offences of illegal access, illegal system interference, illegal data interference and illegal interception. Article 7 establishes as a criminal offence the use of tools to commit offences, applicable to the second phase of identity theft.

4.2. Portuguese law

As regards domestic law, the reference Framework results, first of all, from Act No. 109/2009, of 15 September 2009, the Cybercrime Act, which transposes Framework Decision 2005/222/JHA into our domestic law and adapts the internal law to the Council of Europe Convention on Cybercrime. The following tables show an analysis of the criminal offences set forth in sections 3 to 8 of this Act:

Section number and title	Conducts	Corresponding article of the Council of Europe Convention on Cybercrime
Section 3 - Computer-related forgery	Input, alteration, deletion or suppression of computer data with the intent of causing deception in legal relations or interference, by any other means, in the computer processing of data, resulting in false data or documents, with the intent that they be considered or used for relevant legal purposes as if they were authentic.	Article 7
Section 4 - Damage concerning programs or other computer data	Deletion, alteration, destruction, in whole or in part, damage, suppression or rendering other people’s programs or other computer data non-usable or non-accessible or affecting in any way	Article 4

|||||

4. LEGAL FRAMEWORK

|||||

	their employability, without legal permission or without being authorized by the owner or other holder of the right to the system or to part of it.	
Section 5 - Computer-related sabotage	Serious disturbance, hindering, prevention or interruption of a computer system operation through input, transmission, deterioration, damage, alteration, deletion, prevention of access or suppression of programs or other computer data or through any other way of interference in computer systems, without legal permission or without consent from the owner or another holder of the right on the system or on part of it.	Article 5
Section 6 - Illegal access	To access a computer system, without legal permission or without consent from the owner or another holder of the right on the system or on part of it.	Article 2
Section 7 - Illegal interception	To intercept by technical means transmissions of computer data to, from or within a computer system, without legal consent or without consent from the owner or another holder of the right on the system or on part of it.	Article 3
Section 8 - Illegal reproduction of a program	To illegally replicate, disseminate or disclose to the public a copyrighted computer program.	

|||||

4. LEGAL FRAMEWORK

Section number and title	Conducts	Corresponding article of the Council of Europe Convention on Cybercrime
Section 3(4) - Computer-related forgery	To import, distribute, sell or hold for commercial purposes any device enabling access to a payment means or system, a communication system or a limited access service concerning which the acts prohibited by subsection 2 were committed - input, alteration, deletion or suppression of data recorded or comprised in a bank payment card or in any other device allowing access to a payment means or system, a communication system or a limited access service, generating false data or documents, with the intent that they be considered or used for relevant legal purposes as if they were authentic.	Article 6(1)(a) (b)
Section 4(3) - Damage concerning a program or other computer data	Illegal production, sell, distribution dissemination by any other way or input in one or more computer systems, devices, programs or other computer data aimed at committing the acts prohibited by subsection 1.	
Section 5(2) - Computer-related sabotage	Illegal produces, sells, distributes or by any other way disseminates or inputs in one or more computer systems devices, programs or other computer data aimed at producing the acts not allowed according to subsection 1.	
Section 6(2) - Illegal access	Illegal production, sell, distribution dissemination by any other way or input in one or more computer systems, devices, programs, a executable set of	

4. LEGAL FRAMEWORK

	instructions, a code or other computer data aimed at committing the acts prohibited by subsection 1.
Section 7(3) - Illegal interception	Illegal production, sell, distribution dissemination by any other way or input in one or more computer systems, devices, programs or other computer data aimed at committing the acts prohibited by subsection 1.

Sections 11 to 19 establish rules concerning the procedural right, allowing swiftly collecting and preserving digital evidence, according to the provisions set forth in articles 14 to 21 of the Council of Europe Convention on Cybercrime.

Section 11 starts with establishing the scope of application of the procedural provisions. Thus, sections 11 to 19 apply to offences set forth in this act, to the offences committed by means of a computer system and the ones where there is the need to collect evidence in an electronic device.

Section 12 establishes that, if in the course of the proceedings, aiming at finding out the truth, it will be necessary for evidence purposes to get specific computer data stored in a computer system, including traffic data, that may get lost, be altered or be no more available, the competent judicial or prosecuting authority orders the persons controlling or having such data available, namely the service providers, to preserve the relevant data. Preservation may also be ordered by the criminal police body, by means of authority from the competent judicial or prosecuting authority or whenever faced with urgency or exigent circumstances; the criminal police body shall give immediate notice of that fact to the judicial or prosecuting authority and send them the report set forth in section 253 of the Code of Criminal Procedure. For the persons who control or have such data available, namely the service providers, to execute the order of preservation they must immediately preserve the relevant data, securing and maintaining their integrity for the established time period, in order to allow the competent judicial or prosecuting authority to obtain them, and must assure the confidentiality of application of this procedural measure.

Section 13, aiming at ensuring the preservation of traffic data concerning a certain communication, sets forth that the service provider to which the preservation has been ordered according to section 12, shall inform the judicial or prosecuting authority or the criminal police

4. LEGAL FRAMEWORK

body, as soon as known, of other service providers through which such communication has been made in order to render it possible to identify all service providers as well as he means by which such communication was established.

Section 14 sets forth the imposition for data submission or granting of access to data. Thus, if in the course of the proceedings there is the need, for evidence purposes, to obtain specific computer data stored in a certain computer system, the competent judicial or prosecuting authority orders the persons who control or have such data available, to report them to be joined to the proceedings or to allow access to them, under penalty of being punished for disobedience. This mechanism shall apply to service providers to whom it can be ordered to report data concerning their clients or subscribers, including any information not comprised in traffic data or their contents, held by the service provider in the form of computer data or in any other form. This order cannot be imposed upon a suspect or a defendant in the proceedings. It cannot also be ordered for computer systems used for practicing law, medical and banking activities and journalism. Professional or servant and State secrecy shall apply.

Section 15 addresses computer data search, allowing that, if it will be necessary for evidence purposes aiming at finding out the truth, to obtain certain specific computer data, stored in a certain computer system in the course of the proceedings, the competent judicial or prosecuting authority, shall authorize or issue an order for a search to be carried out in such computer system and, whenever possible, such authority shall preside over the search.

According to section 16 if, in the course of a computer search or of another legal access to a computer system, computer documents or data needed for evidence purposes, aiming at finding the truth, are found, the competent judicial or prosecuting authority shall authorize or issue an order for their seizure. The criminal police body may carry out seizures without prior consent of the judicial or prosecuting authority, in the course of the computer search legally ordered and executed according to the provisions of section 15, as well as in cases of urgency or exigent circumstances.

Section 17 similarly sets forth that if in the course of a computer search or other legitimate access to a computer system in that computer system or in another one, to which legitimate access from the former computer is permitted, electronic mail messages or records of communications of a similar nature are found, the judge may authorize the seizure or issue an order for seizing the data considered to be very relevant for finding out the truth or for evidence purposes; the provisions of the Code of Criminal Procedure concerning the seizure of correspondence shall apply accordingly.

4. LEGAL FRAMEWORK

.....

Section 18 addresses the interception and record of computer data transmissions, which may only be authorized during the inquiry if there are grounds to believe that interception is indispensable for finding out the truth or that it would be very difficult or impossible to obtain evidence in any other way, by means of a reasoned order issued by the investigative judge and in view of a request from the Public Prosecution Service.

Finally, section 19 renders it possible to resort to undercover actions.

Sections 20 to 26 address international cooperation and section 27 addresses territorial jurisdiction and also follow the provisions of articles 23 to 35 and 38 of the Council of Europe Convention on Cybercrime, respectively.

As regards Portuguese law, we must still highlight some of the provisions of the Penal Code that shall mainly apply to cases of identity theft through the Internet: invasion of privacy, set forth in section 192; computer-related invasion of privacy, set forth in section 193; violation of correspondence or telecommunications, set forth in section 194; theft, set forth in section 203; illegal recordings and photographs, set forth in section 199; and computer-related fraud, established by section 221 of the Penal Code. Please see the following table:

.....
PORTUGUESE PENAL CODE

Section number and title	Conducts	Type of crime
Section 192 - Invasion of privacy	To intercept, record, register, use, transmit or disclose a conversation, a telephone communication, electronic mail messages or itemized bills; to capture, photograph, film, record or disclose an image of the persons or objects or intimate spaces; to secretly watch or listen to people who are in a private place or to disclose facts concerning their private life or a serious illness of the victim, without the victim's prior consent and with the intent to invade the victim's private life, namely the victim's sexual or family life privacy.	"Semi-public" [a complaint needs to be filed]

4. LEGAL FRAMEWORK

Section 193 - Computer-related invasion of privacy	To create, maintain or use individually identifiable data files concerning political, religious or philosophical beliefs, political party affiliation or trade union membership, private life or ethnic origin.	"Public" [no need for a complaint to be filed]
Section 194 - Violation of correspondence or telecommunications	To open a parcel, a letter or any other closed writing, addressed to another person, or by technical procedures learn of its content, or to prevent, by any means, that it will be received by the recipient; to interfere in or learn of the content of telecommunications and to disclose the content of telecommunications or closed writings.	"Semi-public" [a complaint needs to be filed]
Section 199 - Illegal recordings and photographs	To record, Without permission, words said by another person, not aimed at the public, even when addressed to him/her; to use or allow the use of the said records, even when illegally made; to photograph or film another person, even in events he/she legally attended or use or allow the use of the already mentioned photographs or films, even if they were legally obtained.	"Semi-public" [a complaint needs to be filed]
Section 203 - Theft	To takes someone else's movable property with the intent of appropriating it.	"Semi-public" [a complaint needs to be filed]
Section 221 - Computer-related fraud	To interfere with data processing results or to incorrectly structure a computer program, to use data in an incomplete or incorrect way, to use data or intervene by any means in their processing, without permission, with the intent of obtaining illicit enrichment for himself or a third party, causing others to suffer a property loss.	"Semi-public" [a complaint needs to be filed]

4. LEGAL FRAMEWORK

4.3. Identity theft, domestic law and the Convention on Cybercrime

Section 3 of the Cybercrime Act – computer-related forgery – and the corresponding article 7 in the Council of Europe Convention on Cybercrime; section 6 of the Cybercrime Act – illegal access – and the corresponding article 2 of the Council of Europe Convention on Cybercrime; section 7 of the Cybercrime Act – illegal interception – and the similar article 3 of the Council of Europe Convention on Cybercrime, as well as articles 4 and 5 of the Council of Europe Convention on Cybercrime, regarding the interference with data and systems, respectively, shall apply to the first phase – obtaining data concerning someone's identity, thus enabling identity theft.

Criminal offences set forth in the Penal Code shall also apply. Invasion of privacy applies to the first phase, as it criminalizes the conducts of intercepting, recording, registering a conversation, a telephone communication, electronic mail messages or itemized bills, of capturing, photographing, filming, registering images of persons or objects or intimate spaces or of secretly watching or listening to persons who are in a private place; these conducts enable obtaining the personal details of a victim. The same happens as regards violation of correspondence or of telecommunications, considering that opening a parcel, a letter or any other closed writing, addressed to another person, or learning, by technical procedures, of its content, or preventing, by any means, that it will be received by the recipient, as well as interfering in the content of telecommunications are also ways to obtain the victim's personal details and other private information. The offence of illegal recordings and photographs should also to be mentioned in the analysis of criminalization of the first phase of identity theft, as recording words said by another person, not aimed at the public, and photographing or filming another person also allows searching for and getting data on the victims. The theft of documents and alike also allows obtaining relevant information for identity theft. It seems that computer fraud can also be included here, as the conducts for obtaining information with lucrative intent are comprised in the core of behaviors this crime aims to punish.

Section 3(4), section 4(3), section 5(2), section 6(2), section 7(3) of the Cybercrime Act and article 6 of the Council of Europe Convention on Cybercrime shall apply to the phase of possession or transfer.

It seems to us that invasion of privacy, by punishing the transmission of electronic mail messages or itemized bills and computer-related invasion of privacy, due to criminalizing the

4. LEGAL FRAMEWORK

act of keeping a file of individually identifiable data, shall also apply.

Any criminal offence corresponding to the offence committed by using another person's identity, shall apply to the third phase – using another person's identity to commit offences.

Invasion of privacy shall apply to this third phase, as it punishes the disclosure of conversations, telephone communications, electronic mail messages or itemized bills; the disclosure of images of persons or objects or intimate spaces; and the disclosure of facts concerning private life or a severe illness of the victim. Computer-related Invasion of privacy shall also apply, as it criminalizes the use of individually identifiable data files concerning political, religious or philosophical beliefs, political party affiliation or trade union membership, private life or ethnic origin. Illegal recordings and photographs are comprised in the core of criminal offences punishing the conducts included in this third phase, as they punish the use or the permission given to use recordings of words said by another person, not aimed at the public, even when addressed to him/her, and photograph or films of another person, even in events he/she legally attended.

Many times computer fraud – section 221 of the Penal Code and article 8 of the Council of Europe Convention on Cybercrime – and illegal access – section 6 of the Cybercrime Act and article 2 of the Council of Europe Convention on Cybercrime – are, the offences applying to this phase of using someone's identification data, namely in cases of phishing.

5.

APPLICATION OF DOMESTIC LAW TO STUDY CASES

[illegible]

5. APPLICATION OF DOMESTIC LAW TO STUDY CASES²¹

< Case 1 >

Section 6(2) of the Cybercrime Act, which punishes the person who sells an executable set of instructions, a code or other computer data for gaining access to a computer system, shall apply to Josué, the bank employee. Section 6(1) of the Cybercrime Act - illegal access - and Section 221(1) of the Penal Code - computer fraud - shall apply to the criminal organization.

< Case 2 >

The criminal offence of illegal interception (section 7(1) of the Cybercrime Act) shall apply to Joana's case, in what concerns the use of keylogging to obtain the data needed for gaining access to Joana's bank account; illegal access (section 6(1) of the Cybercrime Act) and computer-related fraud (section 221 of the Penal Code) shall apply as regards the use of such data to login the online account and withdraw money.

< Case 3 >

Case 3 is not a situation of identity theft, unless the criminal has obtained Jandira's data. Illegal access set forth in section 6(1) of the Cybercrime Act, data interference set forth in section 4(1) of the Cybercrime Act, system interference set forth in section 5(1) of the Cybercrime Act (Jandira could not ordinarily use her computer) and extortion set forth in section 223(1) of the Penal Code shall apply to the described situation.

21 This analysis aims only at mentioning the legal provisions which apply in the depicted cases, for understanding the connection between the existing criminal offences and the conducts analyzed here. We shall not address a possible concomitance that may exist in some cases as regards the applicable legal provisions or how to solve such concomitance.

5. APPLICATION OF DOMESTIC LAW TO STUDY CASES

< Case 4 >

Computer-related forgery, regarding the creation of a fake www site and the setting up of a fake email (section 3(1) of the Cybercrime Act), illegal access, regarding the access to Josefina's online account (section 6(1) of the Cybercrime Act) and computer fraud, regarding the transfer of money from her account into another account (section 221(1) of the Penal Code) shall apply to this study case of phishing.

< Case 5 >

Spamming can be punishable for the crime of system interference (section 5 (1) of the Cybercrime Act) if it impairs the normal functioning of the computer. Computer-related forgery, regarding the creation of a fake email (section 3(1) of the Cybercrime Act) is applicable. The access to José's account is punished by section 6(1) of the Cybercrime Act - illegal access. It seems to us that attempted computer-related fraud (section 221(1) of the Penal Code) was also committed.

< Case 6 >

Jéssica must file a complaint against Joel's behavior and request private prosecution, as his conduct corresponds to the offence of defamation (section 180 of the Penal Code), aggravated by disclosure, according to the provisions of section 183(1)(a) of the Penal Code. Joel imputed facts to Jéssica offending her honor and standing and disseminated such slander through a means facilitating its dissemination. As for the creation of a fake Facebook page it is applicable the crime of computer forgery (section 3(1) of the Cybercrime Act).

5. APPLICATION OF DOMESTIC LAW TO STUDY CASES

< Case 7 >

Joana shall be punished for computer fraud, set forth in section 221(1) of the Penal Code.

< Case 8 >

Julieta was a victim of computer fraud, according to the provision of section 221 of the Penal Code.

< Case 9 >

To the creation of a fake e-mail it is applicable the crime of computer related forgery set forth in section 3(1) of the Cybercrime Act and to the access to Júlio's wife e-mail account it is applicable the crime of illegal access set forth in section 6(1) of the Cybercrime Act. There's also an attempt of computer fraud [section 221(1) of the Penal Code].

< Case 10 >

Jaime, in the possession of the data needed to gain access to Jair's Facebook account, acceded it and posted photographs taken in the scope of Jair's private life, without his consent. The crimes applicable to this case are illegal access [section 6(1) of the Cybercrime Act], invasion of privacy [section 192(1) of the Penal Code] and computerized invasion of privacy [section 193(1) of the Penal Code].

6.

PREVENTION

[illegible]

6. PREVENTION

According to a survey of the European Commission carried out in 2012, 70% of the surveyed population had already heard or seen information on cybercrime, 31% consider themselves to be well informed about the risk of cybercrime and 7% consider themselves to be very well informed²².

Another survey, on 13,000 Internet users in 24 countries, showed that 90% of such internet users delete doubtful email messages sent by unknown persons and 80% use antivirus and do not open attachments or links suggested on messages or emails from unknown persons²³.

Notwithstanding, as regards social networks, only 50% stated to use the privacy options offered by such networks to control the information they share and with whom they share such information, and 35% accept friendship requests from persons they do not know.

Studies carried out on children and teenagers in less developed countries show that this age group has increased risks of victimization. A survey on a population of over 25,000 children of school age from 7 countries in Central and South America shows that from approximately 45% of children who had Internet access at home only 10% had antivirus protection or web filtering on their computers.

States should use their resources to educate the citizens before they will become victims. Educating communities to protect themselves beforehand against identity theft is the most efficient measure to tackle this phenomenon.

6.1. Preventive measures

When using social networks, the user should:

- › Pay attention to the information he/she discloses on social networks: not posting information rendering him/her vulnerable and posting only information the knowledge of which by any person cannot harm him/her;
- › Pay attention to the information that third parties disclose online on himself/herself;
- › Pay attention to the persons to whom he/she gives access to private information;
- › Activate privacy and security options available;
- › Do not accept friend requests from strangers;
- › Know the conditions he/she accepts by joining a social network, which many times include loss of rights over the contents submitted.

22 European
Commission. 2012. *Special
Barometer* 390.

23 Symantec. 2012.
Norton Cybercrime Report 2012.

6. PREVENTION

When using the email, the user should:

- › As regards Portugal, consider that emails written in bad Portuguese – misspelling, grammatical errors, not very coherent sentences or even the use of a mixture of Portuguese and Brazilian Portuguese words – are probably part of phishing scams, even when they come from a known sender; this is the case, for instance, of emails announcing that the user won some sort of prize, that he/she is a finalist in some contest, that there is a problem with the email account or that it is necessary to validate bank data or another system's data;
- › Not do the download of attachments, not click on the links and not reply to emails from unknown persons or having doubtful contents;
- › Try to recognize the address when receiving an email from a bank institution or from any other institution he/she works with;
- › Establish immediate contact with the institution if he/she does not recognize such address, trying to know if the electronic mail message was in fact sent by them;
- › Hover the mouse over any link before clicking it, verifying on the lower left corner of the browser the address where it will be forwarded;
- › Not click on the link if the link domain is external to the domain of the entity supposedly sending the email;
- › Be suspicious of any odd e-mail messages sent by someone you know asking for financial help or for personal data;
- › Avoid using the professional email account for personal use;
- › Not use the electronic mail to send confidential information;
- › Maintain the program used to send electronic mail updated;
- › Switch off the options allowing to automatically open or execute files or programs attached to the messages;
- › Switch off the options to execute JavaScript or other Java programs;

To protect the computer and mobile devices, the user should:

- › Avoid giving rise to situations fostering the theft of computers, mobile phones and tablets, such as leaving them in the car;
- › Protect the computer against malicious users, by using a password to accede and close the session whenever not using the computer;
- › When lending the computer, pay attention to the personal details it may contain,

6. PREVENTION

considering that data recorded on the hard drive may be acceded, even when stored in an account protected with a password;

- › When selling or disposing of the computer, mobile phone or tablet, delete all personal information they may contain;
- › Always keep the computer updated with an antivirus, anti-spyware, firewall e anti-spam protection;
- › Configure the browser used as to block the storage of cookies and pop-ups;
- › Increase the browser security level to medium of high;
- › Always pay attention to the programs installed, verifying their origin – they should originate in the company which created them or in a reliable website;
- › Always verify if the connection to a website is being done through “https” – secure mode – and not “http” – non-secure mode – and, additionally, verify if there is an icon of a lock or a key;
- › In mobile devices, activate the screen protection;
- › Activate the function of remote removal of contents – if there is sensitive information stored in the device²⁴;
- › Make regular security copies of his/her device and have special care with such copies (save them coded with a good password).
- › When installing applications on the device verify if the download is done from a secure and reliable source and pay attention to the type of permissions they request – for example, when an application that shouldn’t need access to the email requests the email access, an alternative should be chosen.

To protect identification documents and personal data, the user should:

- › Carry in his/her wallet only the documents needed for everyday life;
- › Keep his/her wallet in a secure place at work;
- › Keep the documents in a secure place at home, such as a safe;
- › Always destroy physical or digital documents that may contain personal data or other information of the same nature, in order to render impossible looking it up;
- › When doing a request for new checks, request them to be sent to the post office instead of to his/her home;
- › Not have much personal information printed on bank checks;
- › Avoid doing login in websites where personal information is shared from public or open Wi-Fi networks or from unknown computers;
- › Check the legitimacy of the person requesting his/her personal details on the mobile phone

24 There are free applications / services for the different kinds of devices that in case of loss or theft allow deleting all data remotely [applications for Android applications: Mobile Defense or WaveSecure, applications for iPhone: Find My iPhone or MobileMe, among others].

6. PREVENTION

or telephone, by email or by any other means, as well as if such a request is needed:

- » Request the contacting person's identification and the main contact of the entity this person allegedly represents, ascertaining if there is the chance to not supplying any data straightaway by calling back later for that purpose;
 - » Try to think about what the person contacting him/her needs to know: the financial institution with whom he/she works may need to know his/her mother's maiden name to verify his/her identity when he/she calls for obtaining information on his/her account, but when someone calls or sends an email asking his/her mother's maiden name, saying to belong to his/her financial institution, the user should remember that this person does not need to ask such information, as the institution already has it on your file – the aim of such a call or electronic mail message may be simply to obtain information for their own benefit;
 - » If an unknown person calls or sends an email informing that he/she won a prize or any benefit and asks for his/her personal details, the user ask that person to send an application form in writing and if the person won't send it the user break up the contact, if the person sends it, the user should read it carefully and when sending it, make sure it will be addressed to a known and well-reputed financial institution or company.
- › When travelling, give someone he/she trusts in his/her personal information on the phone, be sure that there is no one nearby hearing it;
 - › Inform financial institutions or companies that they should not share his/her personal details;
 - › Save relevant information in files and directories protected with passwords;
 - › Encrypt most important data.

When using the mail, the user should:

- › Try to keep his/her mailbox inviolable, using a good lock;
- › Avoid that correspondence accumulates, thus enabling it to be removed from the place designed for putting it in;
- › When travelling, ask the nearest post office to your address to keep your correspondence or ask a relative, a friend or a neighbor in whom you trust to collect and keep your mail;
- › Try to control the arrival of expected correspondence, in particular containing debit or

6. PREVENTION

- credit cards, bank statements or invoices;
- › If possible, collect and send letters containing personal information or documents at the post office;
- › Interdict the correspondence to be sent to places where he/she doesn't live anymore and ask the post office to forward your correspondence to another place.

To carry out secure financial transactions, the user should:

- › Carry out online financial transactions online through secure websites, with addresses starting with "https:~"; additionally look for a lock or a key next to the address; avoid websites with obvious misspelled words or typing errors and without security references;
- › Check if using the official website of his/her bank – write the name of the bank in the Internet browser to know which is the bank's official website;
- › Remember that banks never ask the user carrying out online operations more than a small part of the numbers (usually three numbers) on the card with the bank credentials;
- › Remember that banks never ask to install applications on mobile phones to increase the security of operations – such applications are usually viruses;
- › End the session when finished using the bank website;
- › In case of doubt call the bank;
- › Keep applications such as Java and Flash updated;
- › Protect all credit accounts with a password.
- › Read the privacy policy of the websites of financial institutions or other institutions with which interaction implies revealing personal data and in case of non-understanding or non-acceptance, consider choosing another institution;
- › When using websites that allow purchases online, check if the wifi network is secure and end session after use; to pay use bank apps that allow the payment of services.

To safely chat online on Instant Messengers, IRC's and Chats, the user should:

- › Use a fake name, not enabling others to identify him/her;
- › Use rooms with a moderator (only applicable to chat rooms);
- › Keep his/her personal information secret;
- › Record chat sessions;
- › Not open email attachments sent from chat rooms.

6. PREVENTION

To create secure passwords, the user should:

- › Avoid predictable sequences when creating a password;
- › Also avoid creating passwords with adjacent keyboard characters. Besides being known, they will be easily identified when typing;
- › Not use personal information linked to him/her or known by other persons, such as date of birth, parts of his/her first name and surname, address, identity or taxpayer numbers, when setting a password;
- › Use passwords with the maximum length allowed, not being words on a dictionary of the Portuguese or other language;
- › Combine letters, numbers and symbols in a non-sequential way;
- › Be creative (think for instance on a sentence with a certain meaning and use the first letter of each word of the sentence as a password);
- › Alternate between lowercase and uppercase letters and lower case letters and replace letters with numbers or symbols;
- › Assign a different password for each service (if there is the need to write down the passwords, keep a written note in a safe place and not a digital note on a computer file);
- › Change passwords on a regular basis.

REMARK: the parents or persons responsible for minors should monitor their online activities, making sure that they take the aforesaid preventive measures.

6.2. Signs of computer infection by malware

When the user's computer is infected with viruses, there is a higher probability for the user to become a victim of identity theft. Thus, it is important to know the signs of a computer infection with viruses:

- › Running slow;
- › Frequent freezes;
- › Pop-up messages, images or strange sounds appearing on the computer;
- › Spontaneous deactivation of protection mechanisms, such as antivirus;
- › Inability of the system to recognize accented vowels;
- › Constant and inexplicable activity on the Internet connection;

6. PREVENTION

- › Changed homepage or favorite search engine;
- › Constant redirection to strange web pages;
- › Emergence of new favorites or toolbars in the browser;
- › Publication of comments on social networks;
- › Establishing conversations in instant messaging (Skype, Google Talk, etc.);
- › Multiple emails returning with failure in reception, which the user does not recognize as being sent by him/her;
- › Emergence of the Java icon on the taskbar without running any applications based on this technology.

6.3. How to identify signs of identity theft

The later identity theft is detected, the more severe its effects can be. Hence the importance for the user to know ways of noticing he/she is being a victim of identity theft and be able to restrain its effects. There are some strategies for a timely detection of this phenomenon.

To timely detect identity theft the user should:

- › Be alert to strange activity on the email account and on the social network profiles;
- › Keep a constant surveillance over all accounts – bank accounts, investment accounts and credit card accounts:
 - » Verify if monthly statements show the last transactions carried out;
 - » See carefully if there are any transactions he/she did not carry out;
- › Verify on a regular basis his/her credit statement to see if there are signs of abnormal activity;
- › Subscribe alerts of activity that the financial companies he/she works with offer;
- › Investigate any refusal of credit – such refusal may be a sign of identity theft and unauthorized use of the account;
- › Immediately contact his/her financial institution whenever being informed on debts he did not make;
- › Keep a file in a safe place with all documents relating to his/her accounts.

7.

CONTAINMENT

[illegible]

7. CONTAINMENT

7.1. Infection by malware

In case of infection by malware, the user should:

- › Disconnect the computer from the network, so that it cannot infect other computers;
- › Clean the computer: cleaning can imply reinstalling the whole system and can be done by the victim, if the victim has a concrete knowledge of the procedures, or by a specialist;
- › When the choice is to clean it, run the cleaning using the “Security Mode” or a CD or pen drive with an antivirus from a non-infected computer;
- › Change all passwords.

7.2. Identity theft

After being a victim of identity theft through the Internet, the user needs to know the means he/she has to contain its effects and to mitigate the impact on his/her personal, social and financial life.

In case of identity theft for committing bank fraud, the user should:

- › If receiving an activity alert from his/her financial institution or if they indicate abnormal account activities, contact the institution immediately;
- › Cancel all credit and debit cards and request the issuing of new ones;
- › Cancel the access to home banking and request new codes;
- › Close the accounts that the criminal might have opened or interfered with;
- › If the identity “thief” has incurred debts or opened accounts in the victim’s name, ask the institution concerned to provide the forms needed to refute having carried out such actions;
- › If there are no specific forms for this purpose, refute it by means of a letter sent to the address specified by the support service;
- › Check with the bank for the possibility of reimbursement;
- › Ask for all credit and debit card statements and search for transactions he/she did not carry out, informing the financial institution whenever coming across any;
- › If errors are found, inform the institution – launch a fraud alert on the credit card statement;
- › Request the financial institution to prevent data on the statement being available;
- › Carefully observe the credit card statement in the years following the identity theft;

7. CONTAINMENT

- › Verify if there is any credit liability assumed in his/her name at the Central Credit Register of the Portuguese Central Bank;
- › File a complaint at the Public Prosecution Service, the Polícia Judiciária [criminal police], the Polícia de Segurança Pública [public security police] or the Guarda Nacional Republicana [national republican guard];
- › Submit a supporting document to the financial institutions confirming that a complaint was filed;
- › Obtain his/her criminal records and verify if the information is correct;
- › Change e-mail password;
- › Cancel the identification documents he/she may have lost;
- › Notify the service companies with whom he/she works, the post office nearest to his/her address, the Social Security and the IMTT [Mobility and Road Transports Institute];
- › Notify possible employers that he/she was a victim of identity theft in case they will be faced with incorrect information on the victim;
- › Keep all emails, SMS or any other communication records between him/her and the crime suspect or perpetrator for evidential purposes.

In case of identity theft for slander on the social network Facebook, the user should:

1. **If the perpetrator creates a fake profile of the victim to post slander contents, the victim should act as follows using Facebook:**
 - › Report the account; in order to do that, the victim should:
 - » Click on the option “...” next to the button “Message” on the right upper corner of the account profile;
 - » From the four options shown, choose the option “Report”;
 - » Then choose option “Report this account”;
 - » Following message will be shown “What is wrong with this account?”, now he/she should click on the option “This timeline is impersonating me or someone I know”;
 - » On screen will immediately appear the following question “Who is it pretending to be?” and the victim should click on “Me”;
 - » The following message will appear “Based on your choices here are some things you can do”, and then he/she should choose “Send to Facebook for review”;
 - » Finally click on the option “Finished”.

7. CONTAINMENT

- › To report contents posted, the victim should:
 - » Click on the arrow pointing down, located at the upper right corner of the posts and choose “I don’t like this post”.

2. If the perpetrator sets up a fake page in the victim’s name to post slander contents:

- › Report the page and the contents posted; for that purpose the victim should:
 - » Click on the option “...” next to the button “Message” on the page upper right corner;
 - » From the five options shown, choose the option “Report Page”;
 - » After that, choose the option “He/she is disturbing me or someone I know”;
 - » Then, the following message will appear “We are sorry you experienced this. Here are some things you can do to try and solve this”, now he/she should choose the option “Send to Facebook for review”;
 - » Finally he/she click on the option “Finished”.

3. If the perpetrator uses the victim’s real profile to post slander contents:

- › Change the access password; for that purpose the victim should:
 - » Click on the icon with a lock on the upper right corner of the blue bar on top of the page;
 - » After that, choose the option “See more definitions”;
 - » Subsequently the victim should click on the option “General” on the upper left corner of that page;
 - » Then on the screen will appear “General account definitions” and on the option “Password” click on “Edit”;
 - » Next, the victim should insert the old password and the new one twice;
 - » Subsequently he/she should choose the option “Save changes”;
 - » After that the following message will appear “Your password has been changed. End session in other devices?” and click on the option “End my session in other devices”;
 - » Finally, the victim should click on “Send”.
- › Delete the posted contents; for that purpose the victim should:

7. CONTAINMENT

- » Click on the arrow pointing down, located at the upper right corner of the posts and choose the option “Delete”;
- » After that the following message will appear “Are you sure you wish to delete this?”, and the victim should choose again the option “Delete”.

4. In any of such cases:

- › Block the perpetrator, so that he/she stops having access to the information the victim posts, as well as all inconvenient Facebook users; for this purpose the victim should:
 - » Click the option “...” next to the button “Message” on the upper right corner of the profile of the user you wish to block;
 - » From the four options shown, choose the option “Block”;
 - » Next will appear the message “Are you sure you want to block ...? “ and the victim should choose the option “Confirm”.
- › File a complaint at the Public Prosecution Service, the Polícia Judiciária [criminal police], the Polícia de Segurança Pública [public security police] or the Guarda Nacional Republicana [national republican guard].

ANNEX

[illegible]

ANNEX

Glossary

Bots and botnets – The term “bot” is an abbreviation of “robot”. Criminals disseminate malicious software (malware) that can transform the user’s computer into a “bot” (robot) or a zombie, as it can also be called. When this happens, the user’s computer may execute automated tasks through the Internet, without his/her consent. Criminals usually use “bots” to infect a high number of computers. These computers form a network or a botnet. Criminals use botnets to send spam messages, disseminate virus, attack computers and servers and also commit fraud and other offences. If the user’s computer is part of a botnet, it can start running slower and the user may be unwittingly helping criminals;

Browser – A program to have access to the Internet, which comes on the computer by default;

Chat – Online conversation;

Cookies – a cookie is a file created by a site to store information on the user’s computer, namely his/her preferences, when the user visits such site. When visiting a site using cookies, the site may ask the browser installed on the computer to put one or more cookies in the hard disk of the user’s computer. Later on, when the user visits the site again, the browser will send the cookies belonging to that site. This allows the site to present information according to the users’ needs. Sites create some cookies so that the user doesn’t need to enter his/her password when visiting the site a second time, for instance. Other sites use cookies to save the user’s preferences;

Computer data – Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

Traffic data – Any computer data relating to a communication by means of a computer system, generated by a computer system that is part of a communication chain, indicating the communication’s origin, destination, route, time, date, size, duration or type of underlying service;

Download – Transfer of Internet contents to the user’s equipment;

E-mail – Electronic mail message;

Flash – Files created by Adobe Flash Player; software usually used for creating interactive animation;

Service provider – Any public or private entity providing their users with the possibility of communicating by means of a computer system, as well as any other entity processing or storing computer data on behalf and to the account of such service provider or their users;

Java – Programming language;

Link – Connection to an Internet site;

Login – The process by which access to a computer system is controlled by identifying and authenticating the user through the credentials provided by such user;

ANNEX

Malware – Any software designed to illegally infiltrate other person's computer systems, aiming at causing damage, alterations or theft of information (whether confidential or not). Computer virus, worms, and spywares are considered malware;

Pop-up – An extra window opening in the browser when visiting a webpage or when opening a certain link;

Computer system – Any device or set of interconnected or associated devices, where one or more of them, executing a program, automatically processes computer data, as well as the network supporting the communication between them and the set of computer data stored, processed, restored or transmitted by such device or devices, having in view their operation, use, protection and maintenance; the definition of computer system on the Council of Europe Convention on Cybercrime includes all forms of technology beyond traditional big size computer systems or working area, such as modern mobile phone, smartphones, PDAs, tablets or similar;

Spoofing – A spoofing attack is a situation in which a person or a program successfully impersonates another one by falsifying data and disguising their real identity, thus obtaining an illegitimate advantage;

Spyware – Automatic computer program, which collects information on the user, his/her Internet habits and transmits such information to an external entity on the Internet, without the user's knowledge or consent. Spyware may be developed by companies that wish to monitor users' habits and make advertisements fitted to their interests, trying to sell their products through the Internet. On the other hand, many viruses carry spyware, aiming at stealing certain users' confidential data, such as bank data;

Website/Site – Internet site or Webpage;

Wi-Fi – Wireless connection to the Internet;

World Wide Web/WWW/Web – An English term, which in Portuguese is literally translated by “teia mundial” [world wide web]; a system of hypertext documents that are interlinked and executed on the Internet.

Support service numbers of the bank institutions which are members of the Portuguese Bank Association

Banco BIG +351 707 244 707	Banif +351 808 200 200	Caixa Geral de Depósitos +351 707 24 24 24
Banco do Brasil +351 707 222 500	Barclays +351 707 50 50 50	Deutsche Bank +351 808 201 251
Banco Carregosa Porto - +351 22 608 64 64 Lisboa - +351 21 013 41 00	BBVA +351 707 256 256	Millennium +351 707 50 24 24
Banco Finantia +351 707 788 080	BNP Paribas +351 21 791 02 00	Montepio +351 808 20 26 26
Banco Invest +351 800 200 160	BPI +351 707 020 500	Novo Banco +351 707 247 365
Banco Popular +351 808 20 16 16	Caixa Agrícola +351 808 20 60 60	Santander +351 707 21 24 24

[illegible]

[illegible]

10000101010010101010010101001000011001010101010100101010101000000101010101010001
01010101010001111101010101010101000010101001010101001010100100001100101011010101010
0101Project developed in partnership by:1000111101010101010101000010101001010101010100



11110
10100101010100101010010000110010101101010101001010101010000001010101010100011111010
10100011111010101010101010000101010010101010010101001000011001010110101010100101010
0101> Associação Portuguesa de Apoio à Vítima10101010101000010101001010101001010100
1010 [Portuguese Association for Victim Support]0000010101010101000111110101010101
1111> Fiscalía General del Estado de España - Unidad Especializada contra la1010000
0101 criminalidad informática11111010101010101010000101010010101010010101001000011
1010 [Spanish General Prosecutor's Office - Cybercrime Specialized Unit]01010101000
1010> Politia Romana000000101010101010101000010101010100101010101010100000010101
1010 [General Inspectorate of the Romanian Police]10101010100101010010000110010101
1000> Pärnu Lähisuhtevägivalla Ennetuskeskus- Varjupaik1010101010100001010100101010
0101 [Pärnu's Centre of Gender Based Violence - Estonia]101010100000010101010101010
0010> Polícia Judiciária0010101010101001010100100101010101010101010100001010101010101
0010 [Portuguese Judiciary Police]01010101000101010101001010101010100001010100101010
0101> Procuradoria Geral da República1101010101001010101010000001010101010100011111
0101 [Portuguese General Prosecutor's Office]010101010010000110010101110101010100101
10101010100101010101000000101010101010001111101010101010101000010101001010101010
0101010100101010100100001100101011010101010010101010101000000101010101000111110101010
101000101010010000110010101101010101001010101010101000000101010101010001111101010101010
111010101010101010000101010010101001010100100001100101011010101010010101010100000
1010101010000001010101010100011111010101010101010000101010010101010010000110
01010010000110010101101001010100100001100101011010101010010101010100000010101010101
00010101010101010001111101010101010101000010101001010100101010010000110010101101010
10010101101010101001010101010100000010101010101000111110101010101010000101010010101
001010100101010101001000110010101101001010100100001100101011010101010010101010101
1010ISBN 978-972-8852-78-8101010100011111010101010101010000101010010101010010101001
01010010101001000011001010110101010100101010101000000101010101010001111101010101010
1110Reproduction, quotation and/or reference with informative and001111101011001010
0100non-commercial ends are allowed if the source is mentioned. The European001010101
1010Commission disclaims any liability regarding the content of this document.10101
0001The responsibility for the accuracy of the information rests with its0111101001
0100authors.01010101010100001010100010101010101010100000010101010101000111110101
01000111110101010101010100001010100101010100101010010000110010101101010101001010101
1010Project promoted by the Portuguese Association for Victim Support (APAV)0101001
0101and co-funded by the Prevention of and Fight against Crime Programme of00001010
0101the European Union.011111010101010101010000101010010101010010101000011001010
010000110010101101010101001010101010000001010101010100011111010101010101000010101
101010010101010100000010101010101000111110101010101010000101010010101010010101001