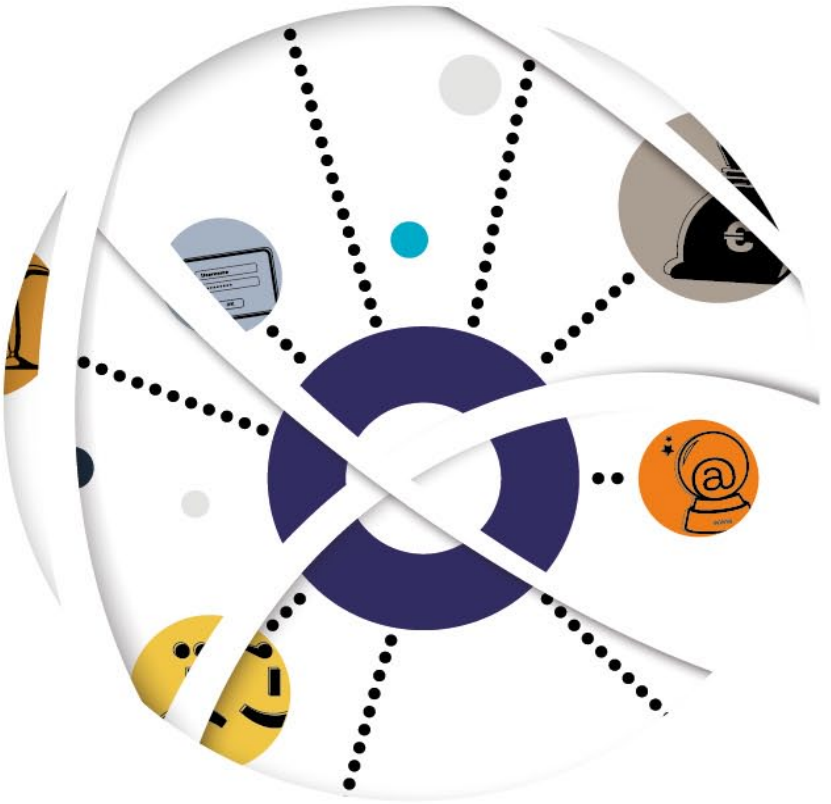
SAFE WEB EXPLORE

BE INFORMED.
BE SAFE.



Hellenic Republic
Ministry of Interior and
Administrative Reconstruction

HELLENIC POLICE HEADQUARTERS

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#Internet_also_carries_risks

#evolution_of_Internet

#legislation_on_the_Internet

#cyberbullying

#social_media_&_facebook

#child_pornography

#Industrial_espionage

#Internet_fraud

INDEX

#Internet_also_carries_risks

Learn how you can recognize them and protect yourself or your family from cyberbullying, personal data theft and other risks.

NEGATIVE ASPECTS OF THE INTERNET!

Child Pornography
Individuals above suspicion gain the trust of children, provoke sex-related discussions, and send inappropriate pictures as something acceptable and normal.

Digital Bullying
Harassment, defamation, spreading false rumors from people trying to psychologically control their victims.

Chat Rooms
The use of aliases allows anonymity. The illusion of safety, however, can transform online contacts into one of the largest and most dangerous pitfalls of the Internet. The only true friends are in real life and are tested in the real world and in real time.

Financial Fraud
E-mails with deceptive content, promising huge inheritances, passwords' and credit card pins' theft, exorbitant charges, and fraudulent purchases: some persons might use the Internet trying to mislead you.

Violation of Personal Data
Bombardment with advertising messages via the Internet, excessive use of surveillance cameras, violation of health and financial data, stolen passwords and photos from user accounts on social networking sites.

Suicides
In five years over 378 people have expressed their intention to commit suicide.

Social Networking Sites
The conditions of use indicate that users waive their copyright for content uploaded in social networking websites. Also, there is no guarantee for the security and privacy of applications.

Internet Addiction
Internet addiction is an ever-growing contemporary phenomenon, which mainly affects adolescents or adults who first come in contact with the Internet and have not developed resistance. It is a relatively new form of dependency, which lures adults and children into another reality, creating alienation and obsession. As a result, they neglect their obligations, show indifference for the real world, or even suffer from headaches and eye-dryness, caused by long hours in front of a computer.

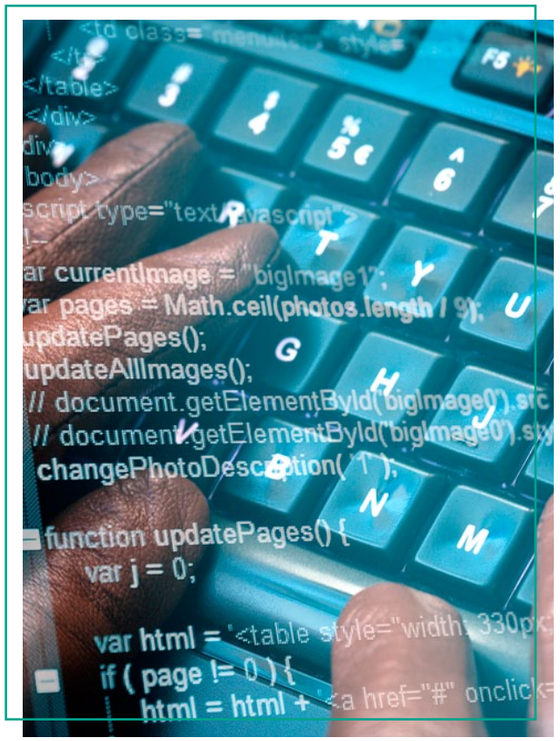
Proper Use of the Internet
Do not stop using the Internet, but learn to set limits, and engage in other activities away from your computer. One day offline may be more interesting and more fun. One hour per day on the Internet is considered sufficient for online information and entertainment. Do not forget that the time you spend in front of a computer is usually taken from someone you love.
The parents' role is very important in the prevention and confrontation of the addiction of children on the Internet. As regards prevention, the most important thing the parents need to do is to know themselves the Internet, in order to effectively control its use by their children.

TIPS FOR PARENTS!

- Prefer to place your computer in areas such as the living room and not in the child's bedroom, so that you will be able to supervise your child, without him or her feeling being controlled.
- Make surfing the Internet a family activity. Use the computer with your children.
- Tell your children about the dangers of chatting with strangers in chatrooms.
- Talk to your children about safety when surfing the Internet (contact with dangerous people or access to sites with harmful content). Teach them not to give out personal information without your permission (surname, name, age, home address, phone number, family income, school timetables, names of friends, etc.).
- Do not give your credit card to children for online transactions.
- Never allow your children to meet in person with people that they got to know online. Explain that strangers with whom they want to meet may be dangerous.
- Use "filters", i.e. specific software products designed to prevent access to unwanted sites (violence, pornography).
- Check the content of audiovisual material such as CDs, diskettes and others that your children buy or share with friends.
- Stay close to your children and engage in all their online activity, in the same way you do for school activities.
- Talk with your child and explain that if something unexpected or annoying occurs online, they need to close the web page.

TIPS FOR KIDS!

The Internet educates and entertains. However, it can create problems if it is used irresponsibly. That is why:
- Do not give to anyone, even to your best friend, your online passwords. The only people who should know your passwords are your parents.
- Do not respond to e-mails that make you feel uncomfortable. If you receive such a message, do not hesitate to tell your parents or a person you trust.
- If you feel uncomfortable while chatting in a chatroom, stop the conversation immediately .
- Avoid sending over the Internet photos of you and your personal information to unknown persons.
- Be sure about your acquaintances on the Internet. Remember that the people you know may not be what they say they are!
- If someone harasses you, remember that you can get out of the site with a simple "click"!
- Think very carefully before you decide to meet in person someone you met on the Internet. Ask the opinion of your parents about this subject.
- If you decide to meet with your "online friend", inform your parents or someone you trust, and arrange this meeting to be in public.
- Do not immediately trust what you see on the Internet.
- Talk to your parents about what you see and experience when "surfing" on the Internet.



INTERNET: A WORLD MIRACLE!

The Internet is a world computer network interface characterized as one of the modern wonders of the world, as it is among the most essential tools in everyday life, and gradually affects every human activity. It is a window to the world that offers countless services at very low cost! Let's see together the positive aspects of the Internet! The Internet has revolutionized communication, minimizing its costs and increasing its speed. Distances are eliminated, and people can talk to their friends and old classmates worldwide, directly and interactively with the push of a button! Also, they can publish freely their texts, exchanging views on all sorts of subjects! However, the most spectacular opportunity offered by the Internet is web-browsing and gathering information from different websites: users can visit these sites and be informed on issues that interest them, on services offered, on products they want to buy, on educational institutions, on laws and regulations, government agencies, and more. Also, with just a "click" from the comfort of his home, the user can consult appropriate sources or books that were not previously immediately available, and thus find within a few seconds information on any topic of his or her interest!

The Internet's possibilities are particularly important in the domain of education and training. More and more libraries feature on-line catalogs of their books. Those interested can locate the book they need with the help of a search engine, while some libraries even allow on-line book borrowing. Innovative and effective teaching methods employ the Internet and contribute to the best knowledge and learning through advanced tele-education systems.

Also, the Internet facilitates everyday life. Via the Internet many people make purchases, arrange banking issues, and generally carry out tasks that would otherwise require lots of time.The possibilities offered by the Internet concern equally professional life, since using the Internet anyone can work away from the traditional workplace. Some professionals resort particularly to this new form of work, telework (writers, journalists, translators, etc.).

Through data digitization, we can find in just seconds public documents concerning our person, submit applications and send documents, saving time, effort and money. Using the Internet, we can travel in any country with a "click", get to know foreign cultures, see images from other countries, and read about other countries' history! Furthermore, we can organize our trips, by booking tickets and hotels at low prices, reading travel experiences of other people, and writing our own!

But the Internet is not only for young people. The use of new technologies facilitates the daily life of the elderly and, on top of that, according to studies' results, browsing the Internet may help improve cognitive function and has a positive effect on depression and the feeling of loneliness.

Finally, through the Internet we have fun: we can play games, listen to songs, find interesting pictures, book cinema tickets, and all these from the comfort of our home!

Our Service recommends:

[YES TO THE INTERNET BUT WITH CONDITIONS!]

USEFUL LINKS

Useful tips from Cyber Crime Division:
http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=

Children's Rights Protection Organization:
http://www.hamogelo.gr

Cyber Crime Division webpage:
www.cyberkid.gr

Cyber Crime Division Facebook:
www.facebook.com/cyberkid.gov.gr

Adolescent Health Unit Second Department of Pediatrics University of Athens:
www.youth-health.gr

Hellenic Association for the Study of Internet Addiction Disorder:
www.hasiad.gr

#evolution_of_Internet

assessments and projections

INTERNET

The Internet is the largest computer network in the world, which allows communication and exchange of information all over the planet. It has been described as the greatest “invention” of all times. In just a few decades it has conquered the whole world and now it constitutes the largest civil society organization worldwide.

The Internet is a parallel “virtual” community which abolishes every social and cultural division of the real world that the traditional media are not able to overcome. The Internet, as opposed to traditional media and communication, makes possible to experience a two-way communication and enables all users to participate directly, getting and disseminating information. The Internet is abolishing the borders and eliminating the distances, favoring communications in the eternal conflict between transport and communications.

CHRONOLOGY

The truth is that the Internet is present in our daily life the last decades, during which it has experienced an explosive growth and became the most important element in the evolution of mankind from the industrial age into the information age and the digital revolution. Important stages in this evolution were the following:

- **1969:** The ARPANET, the ancestor of today’s Internet, is created, bringing together four mini computers from respective academic institutions in the USA, who were connected at speeds up to 50kbps.
- **1972:** The idea of the e-mail is introduced to the public, when the ARPANET interconnects 23 computers.
- **1974:** The first study on the TCP (Transmission Control Program), which allows communication between different computer networks, is published by V. Cerf and B. Kahn.
- **1974:** Inauguration of the Telnet, the first commercial version of ARPANET.
- **1982:** First use of the term “Internet”, defined as a connected set of networks using the protocol TCP/IP.
- **1986:** Creation of the National Science Foundation Net (NSFNET) which interconnects all the universities of the USA.
- **1990:** Creation of the first Internet provider with the name “The World comes on-line (world.std.com)” that offers Internet connection via telephone.
- **1990:** Greece is connected to the Internet through the network NSFNET.
- **1991:** CERN presents the World Wide Web, which introduces to the public the idea of using the Internet to provide information via hypertext pages (hypertext).
- **1993:** The first web browser (Mosaic) is presented by the company National Center for Supercomputing Applications (NCSA).
- **1994:** Banking services are offered for the first time via the Internet (Stanford Federal Credit Union).
- **1996:** The first mobile with Internet access (Nokia 9000 Communicator), weighing 397g, becomes commercially available!
- **2008:** Google announces that the list of URLs exceeded 1 trillion.

TODAY

Since the four computers that originally constituted the ARPANET, the massive expansion of the Internet becomes obvious by looking at the current numbers. In 2012, Internet users exceeded 2 billion worldwide, which amounts to 30.2% of the world population. Similarly the proportion in Europe is 58.3% and in North America 78.3%! It is worth mentioning that the increase of users worldwide in the past 10 years exceeded 450%.

The web (World Wide Web) now totals almost 50 billion websites. Social networks are growing rapidly with Facebook ranked first, surpassing 1 billion users, and YouTube reaching one trillion video playbacks.

TODAY

The development of the Internet in Greece offers a similar picture. Internet users are more than five million (>50% of the population), showing an increase of more than 250% over the last decade. Similarly, broadband users surpassed 2,500,000 and Facebook users approached 4 million. Interestingly, in the 13-24 age group usage rate reaches 90%, indicating the further rapid development of the Internet.

In its current form Internet is varied, providing a multitude of services that cover a wide range of daily needs:

- Knowledge
- Education
- Information
- Contact
- Update
- Entertainment
- Recreation
- Shopping
- Travel

WHAT WE SAW IN THE LAST DECADE

In the past decade a series of technological developments and social trends established the current form of the Internet. Examples were:

Social Media: The most important aspect of the Internet's evolution over the past decade was undoubtedly the explosive growth of social media.

Video sharing: With broadband available to almost every home and speeds that increase significantly, video sharing became practically feasible, and YouTube and its services became part of everyday life.

Mobile Internet – 3G – smartphones: A very important development was that access to the Internet from mobile devices has been made possible and affordable for everyone, Internet users being able to stay connected from any location and any device.

Online gaming: Online games gained rapidly a large number of users. Huge virtual worlds attract daily a large percentage of users with some of the online games being played by more than 10 million users.

Internet radio: The classic radio mutated heavily online, earning many admirers and abolishing transmission borders worldwide.

Blogs: Blogs were one of the latest trends of the past decade, giving stage for expression to all and winning every day millions of fans.

WHAT WE EXPECT TO SEE OVER THE NEXT DECADE

Based on previous developments, the samples which have been presented and the growing tendency to development, in the next decade we expect new innovative solutions and services. Let's take a look at some of the issues that are expected to amaze us in the years to come:

Cloud: The "cloud" has already emerged in the global market by opening new ways of access to data and services. This information now becomes accessible from anywhere and from any device that has Internet access. Services do not require installation, diminishing thus computing power requirements both for individuals and for companies. In the next decade we expect more and more services migrating to the "cloud" and the emergence of online operating systems, text editors and other everyday tools, which will be available exclusively as cloud services.

3D Internet: With monitors already supporting 3D viewing, soon the Internet will have 3D websites and applications, and 3D objects will replace the current videos and photos, giving a new face to the Internet.

IPTV: All new television sets have an Internet connection, and broadcasting services over the Internet now cover all the needs for image transmission. Based on the above and following the radio example, TV is expected to mutate, maybe entirely, to Internet TV.

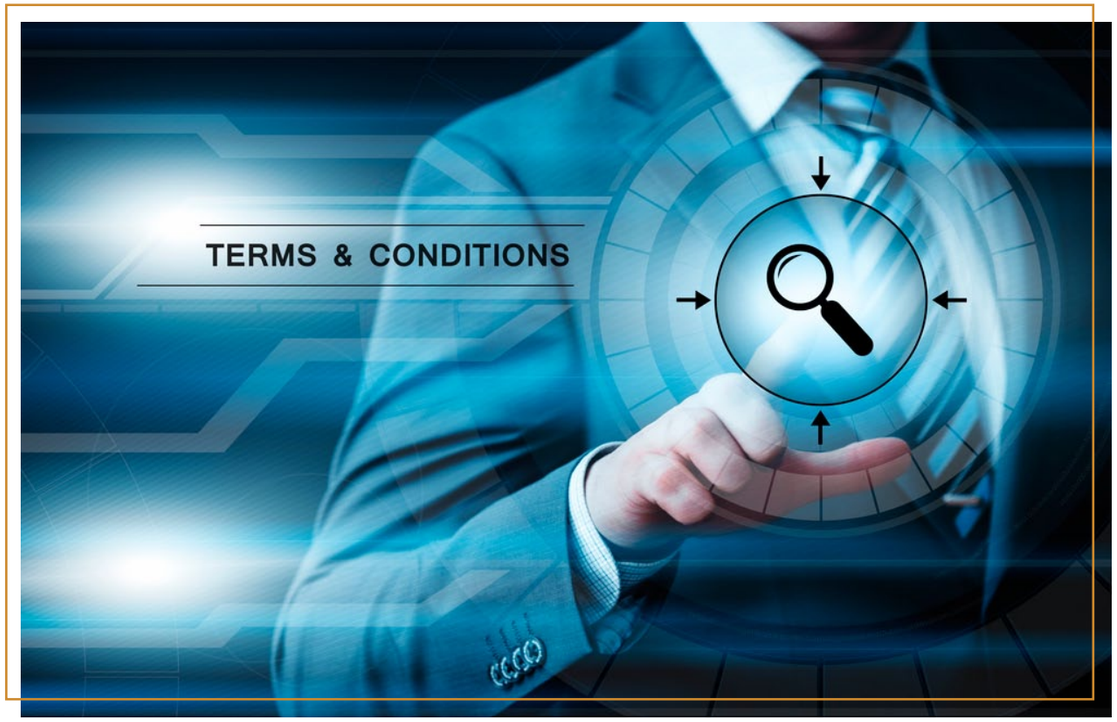
E-learning – tele-working: These two applications of the Internet are expected to come to the fore, reducing travel costs and corporate support costs.

Nanotechnology: Nanotechnology has already applications in many fields, and recent experiments show that devices such as molecular computers are no longer a pipe dream. It is conceivable, then, that very soon users will have powerful PCs in a wristwatch or a simple handset.

Full interface: Following the prediction of Bill Gates («every device in the world will be connected») and with IPv6 already put in place in some European countries, soon all devices will be interconnected in a hyper-connection that will include household electrical appliances, automobiles, mobile phones and any portable or home device.

4G → 5G and beyond: By 2009 the 4G became a reality. With advances in mobile broadband galloping, the next generations of mobile networks will not be long to follow.

legislation
_on_the
_Internet



In Greek legislation, there is no specific law referring exclusively to Internet-related issues and regulating the behavior of Internet users from the aspect of the Penal Law.
Most of the offences that are described and punished by the Greek Penal Code may nowadays be committed by electronic means (computer crimes) as well as via Internet. In these cases the provisions of the Penal Code or specific Penal Laws are mutatis mutandis applicable.

PENAL CODE

Article **292A** "Crimes against the security of telephone communications"
Article **348A** "Pornography of minors"
Article **348B** "Attracting (grooming) children for sexual purposes"
Article **348C** "Pornographic performances of minors"
Article **361** "Insult"
Article **362** "Defamation"
Article **361** "Libel"
Article **370** "Violation of the correspondence (mail) secrecy"
Article **370A** "Violation of the secrecy of telephone communications and of oral conversations"
Article **370B** "Violation of computer data or programs which are considered as secret"
Article **370C** "Illegal copy or use of computer programs and illegal access to computer data"
Article **385** "Extortion"
Article **386A** "Fraud via computer"

LAWS AND PRESIDENTIAL DECREES

Electronic Communications - Telecommunications

Law 2867/2000 "Organisation and operation of the Telecommunications Sector"
Law 3431/2006 "About electronic communications and other provisions"
Law 3783/2009 "Identification of the owners and users of mobile telephony services equipment and other provisions"

Intellectual Property (Copyright)

Law 2121/1993 "Intellectual property, related rights and cultural issues"

Personal Data

Law 2472/1997 "Protection of the person from the process of personal data"
Law 3471/2006 "Protection of personal data and of private life in the sector of the electronic communications and amendment of the Law 2472/97"

Games (gambling)

Law 4002/2011 "Regulation of the gaming market"
Law 2433/1996 "Regulation of issues related to OPAP and other provisions"

Confidentiality of communications

Law 2225/1994 "About the protection of the freedom of correspondence and communication" as amended until today
Law 3674/2008 "Strengthening of the institutional framework of securing the confidentiality of telephone communications and other provisions"
Presidential Decree 47/2005 "Procedures and technical and organizational guarantees for the lifting of confidentiality and for securing the confidentiality"

Data Retention

Law 3917/2011 "Retention of data produced or submitted to process in light of providing publicly available electronic communications or public networks communications services, use of surveillance systems by receiving or recording sound or images in public places, and related provisions"

According to the Law above, the companies which supply Internet services **do not** keep information concerning the subscribers and data which correspond to electronic traces, beyond the period of twelve (12) months from the date of the communication.

Electronic Commerce

Presidential Decree 150/2001: "Electronic signatures"
Presidential Decree 131/2003: "Electronic commerce etc."

Combatting certain forms and expressions of racism and xenophobia by means of criminal law and via Internet

Law 4285/14 "Amendment of the Law 927/1979 (A΄ 139) and adaptation to the framework decision 2008/913/JHA of 28th November 2008, about combatting certain forms and expressions of racism and xenophobia by means of criminal law"

OPINIONS

- **Opinion No. 9 of 29-06-2006 of the Public Prosecutor of the Supreme Court Mr G. Sanidas**, where it was clarified that: 1. The confidentiality of the communications does not cover **a)** the communication via Internet, and **b)** the external information of the communication (name and surname and other information concerning the subscribers, telephone numbers, time and place of calls, duration of calls etc.). **2) The prosecuting, investigating and enquiring authorities and the Judicial Councils and the Courts** have the right to ask the providers of communication services via Internet for the electronic traces of a criminal action, including the day, the month, the date, the information concerning the person to whom the trace corresponds, and also the providers of other communication services for the "external information" of the communication. The provider is obliged to submit this information without prior permission of an Authority and especially ADAE (Authority for the Security of the Communications Confidentiality). 3) ADAE, as well as any other independent authority, is either entitled or has the right to examine in any way, directly or indirectly, whether the decision of the judicial bodies about the lifting of the confidentiality is according to the law or not.
- **Opinion No. 12/2009 of the Public Prosecutor of the Supreme Court Mr I. Tentes**, by which the position of the Public Prosecution of the Supreme Court of Appeal on this matter was consolidated. More specifically, in this last Opinion on this matter the following interesting details are mentioned: **a)** The cases that are of interest on this issue, that is the cases where the **investigation authorities** ask the providers of electronic communications services to communicate data related to the user's identity or the connection's location, so as to spot the offender of insulting, defamatory, threatening, extortionate telephone calls or messages, during the procedure of **preliminary examination, investigation or main investigation**, after complaint usually by the victim, recipient of these calls etc., {these cases} fall out of the protective scope of the provision of Article 19, paragraph 1 of the Constitution. In the cases above there is not a question of communication or response within the meaning of the constitutional provision. These contacts, by their specific purpose and content, which is directly criminal (Karras, Penal Procedural Law, no. 705), on the one hand do not constitute "exchange of opinions, thoughts etc." and on the other hand are not being made within the frame of a relationship of intimacy and confidentiality (Chrysogonos, above, p. 260, Tsakyrakis, above, p. 997, 998). Therefore, there are no grounds for the justification of confidentiality protection , that is the protection of the person from the danger of violation of his/her personal freedom, in the broad sense, and his/her entrapment by means of exposure to any kind of consequences from any excessive and reckless expressions during private and confidential communications, and therefore the communication of this kind is not protected by the Constitution and consequently by the provision of the Article 4, par. 1 of the Law 3471/2006. **b)** Accordingly, the investigation authorities, responding to the protective duty of the State, expressed as a positive obligation to secure the unhindered and effective exercise of the rights of the person, according to the Article 25, paragraph 1 of the Constitution, and acting according to the constitutional requirement for the provision of remedies (Article 20 of the Constitution) and for the punishment of crimes (Articles 96, par. 1, and 87, par. 1 of the Constitution), {the authorities} can, within their right to collect the necessary evidence for the certification of the crime (Articles 251, 239, par. 1-2 and Article 248 of the Code of Penal Procedure), ask for the abovementioned information, without previously following the procedure of lifting of the confidentiality, of the **Law 2225/1994 implementing part of the provision of the Article 19, par. 1, subpar. b of the Constitution**, since, as it was said, there not a matter of confidentiality. **c)** It is self-evident that the **main investigation or preliminary examination or investigation** must be carried out after an order from a prosecutor, as well as that **the delegated investigator or the ordering prosecutor**, according to the fundamental principle about the investigations, will ask for the information above after, having followed the principles of proportionality, he/she judges that, based on the information available by that time, only by these means the certification of the crime and the discovery of the offender will be possible (Karras, above, no. 44)..."
- **Opinion No. 9/2011 of the Public Prosecutor of the Supreme Court Mr A. Katsirodi** (confirms what is mentioned above)
- **Opinion No. 5058 of 14-12-2012 of the Public Prosecutor of the Supreme Court Mr I. Tentes**

Rulings

New **Regulation of management and allocation of domain names ending to .gr** - Decision 750/2 (19-02-2015) of the **National Telecommunications and Post Commission** (EETT), entered into force from 24th March 2015.

TREATIES

Budapest Convention

The offences which take place on the Internet cause a lot of legal problems due to the complex operation of the **computers** and due to the specific characteristics of the **Internet**.
These are exactly the problems that the **Convention on Cybercrime** attempts to solve.

This Convention on Cybercrime, which was signed by the Council of Europe on 23 November 2001 in Budapest and which, it should be noted, has not yet been ratified by Greece, attempts to develop a common anti-crime policy and the contracting states adopt legislative measures, so that cybercrimes are addressed jointly.

#cyberbullying

when psychological violence on
the Internet threatens every child

WHAT IS CYBERBULLYING?

You or a friend of yours have received or seen an altered photo of you on the Internet, or you have accepted an offensive message. All the above **constitute digital harassment** and, however funny they might be for the people that created or have seen them, they are not funny at all for the people offended, as they have major consequences to their life.

Digital bullying (cyberbullying) is **any repeated act of intimidation, aggression, harassment, terrorizing or authoritarian behavior through the use of digital devices (PC, mobile phone, tablets)**. It is an incorrect and unacceptable behavior that should in no way be overlooked or ignored.

Cyberbullying is much like the simple and well known bullying that many may have experienced once in their life. It is like intimidation since there is a perpetrator, a victim and an observer. But there are also differences, such as:

- It can reach multiple recipients in a very short time.
- It is practically impossible to pre-check electronic messages.
- The perpetrator feels that he or she can remain anonymous.
- The lack of personal contact with the victim makes the offender harsher.
- The victim is affected at home and at his personal space.

Cyberbullying may occur through:

- E-mail
- Text messages (SMS)
- Social media
- Chat rooms
- Blogs
- Online games

How cyberbullying takes place

Those who engage in cyberbullying usually tend to use new technologies to harass, threaten, intimidate, discredit and, in some cases, impersonate others or steal their identity. Some of the most common methods are:

- Sending a text, an e-mail, or instant messages with offensive content (in instant messengers or chatrooms).
- Malicious uploading of photos in social media, blogs or other websites with the sole purpose of harassment.
- Spreading rumors and false facts to discredit someone to third parties in social media, blogs, websites, etc.
- Anonymous calls and messages aimed at generating fear and anxiety.
- Using someone else's user name to spread rumors and false facts concerning other people (identity theft).
- Creating websites targeting specific people and inviting others to post hate messages.
- Intentionally sending Trojan horses programs to cause trouble by intercepting passwords.
- Intimidating during an interactive game.

PERPETRATOR'S-VICTIM'S PROFILE

Anyone can be victim, perpetrator or, more often, an observer of cyberbullying.
Cyberbullying might attract children who have never harassed anyone in real life, because they think they are anonymous when using Internet or their mobile phone. In the cyberspace the perpetrators can do things that they have never thought of doing face-to-face, and they can also use new technologies to intentionally disturb a friend, a stranger, even a teacher. Sometimes they may even give in to peer pressure and forward an e-mail with intimidating content without considering the consequences of this action.

Why would anyone intimidate an individual through the Internet?

- Need for power
- Anger
- Jealousy
- Entertainment
- Psychological repression
- Retaliation
- Need for attention

What do the victims feel?

- Anger
- Indignation
- Grief
- Shame
- Fear

Consequences

Cyberbullying seems to be an innocent joke but it can actually have very serious consequences, such as:

- Absence from courses or lessons
- Sudden drop in school performance
- Performing acts contrary to the child's character or illegal acts due to blackmailing
- Depression
- Suicide

The case of 13-year old Megan from the US, who suffered depression and committed suicide after her web-friend Josh "ditched" her, is typical. As it turned out, her "boyfriend" was actually the mother of a friend with whom Megan had argued.

Ways of action

Avoid responding to the perpetrator's threats. Responding aggressively brings new threats and satisfies the perpetrator's needs or allows him or her to continue harassing you.

- Change your e-mail account or shut down your social media page – if possible create new accounts.
- Keep evidence of the perpetrator's activity, including as many details as possible, such as dates and times, e-mail accounts etc. It is advisable to have this evidence in printed form also.
- Remove from your "friends" list any individual that harassed you, and set your social media profile to "confidential", if it is not already.

PERPETRATOR'S-VICTIM'S PROFILE

- If you know the perpetrator, ask him or her to erase the messages and restore the truth in case he or she has spread rumors. It is important to inform the child's parents for his or her behavior in order to contain the perpetrator.
- If the harassment takes place in a social networking site (e.g. Facebook), report the incident as soon as possible to the website operators.
- If you notice that someone intimidates someone else on the Internet, report the intimidation to your parents – do not stay silent!
- In every case you should talk immediately to your parents or your teachers, or call the Cyber Crime Division. **Don't be afraid - You are not alone!**

If the bullying takes place via a social networking site or chat room:

- **Facebook:** If someone bothers you on Facebook, please report it by clicking the "Report / Block" button located on your profile. In the report menu you can specify your reasons for reporting, e.g. someone represents you (identity theft), or threatens you. You can also choose to block any user who is bothering you so as to not receiving his or her messages. A good safety guide for children and parents can be found at **www.facebook.com/safety.** Also, at **www.facebook.com/help/215543298568604/** you can find out how to restore a "stolen" Facebook account.
- MySpace: Relevant safety guide in.
- YouTube: You can report a malicious video by clicking on the "Report" button located under the video.
- Instant messaging: MSN-Yahoo: By selecting "Help tab" you will come up with multiple choices, one of wich is "Report Abuse".
- Chatrooms: In their vast majority moderators are usually very strict with cases of malicious attack. It would be advisable to contact them by e-mail stating the specific problem.

PROTECTION MEASURES

- Privacy in social networking sites. You should restrict information concerning you or your family. By doing this, you reduce the chances of falling victim of unidentified perpetrators.
- You should not become friend with everyone on social networking websites.
- Treat others online as you would in real life. If someone becomes disrespectful or rude, you do not have to answer. He or she will understand that you are not responding and stop sending insulting messages. If these messages persist, seek assistance from a trusted adult.
- Never open an e-mail sent by someone you do not know.
- Delete strange e-mails or text messages from people you do not know. If in doubt, seek advice from a trusted adult.
- "Google yourself!". Use a search engine regularly and search your name or the nickname that you use on the Internet. This way you can supervise your virtual presence.
- You do not need to be "always connected". Disconnect and turn off the computer. Give yourself a break. Do not stay online for too long.
- Do not use passwords that are easily guessed (date of birth, etc.).

The Greek Cyber Crime Division does not incriminate the children's smile. Children's misunderstandings are not cyberbullying. Cyberbullying victims feel terror, anxiety, despair, they are on the edge. According to the Division's findings children are not terrified, but full of life and confidence, and know what they want. The key is information and education through schools, so that children understand that the Internet is not anonymous. Everyone has his or her own Internet identity, which can be traced.

social_media_ &_facebook

risks and advice concerning the Internet's social networks

WHAT ARE THE SOCIAL NETWORKING WEBSITES

They are websites which offer to their users the ability to create their own personal profile, introduce themselves and communicate with other users online. These users can be real life friends or perfect strangers.
Through this online way of communication online communities were created, where people with common interests can share information and discuss about their point of view or ideologies. Usually those social networking websites bring people close due to their similarities.

Nowadays, it is not hard for somebody to create a profile because it does not require particular technical knowledge in order to have a profile and upload comments, photos, and videos which later on will be viewed by other users as well.

In Greece the most popular and well-known sites with the most views and users are the following: Facebook, Twitter, MySpace, and YouTube.

As in the case of the Internet in general, **we say YES to the use of Social Media Networking**. But, before we start anything or get involved with the social media, it is essential to acquire knowledge around some major safety rules and to be aware of the impact of Internet. This will be achieved only through the development of critical and perceptual ability, and from the ability to recognize and identify the risk which can occur through our browsing into social media.

HIDDEN RISKS IN SOCIAL MEDIA NETWORKING

Use of the information for any other purpose

In social networks the users have a false belief concerning the notion of privacy in their personal information they share. They tend to believe that the information they will upload is only available to their family and friends. In fact, other users can have access to your personal information and might use it against you to hurt you or to cause you a problem which will affect your daily life in and out of the Internet. For example, a comment which is meant to be for a friend of yours could be easily read from your employer and it could be responsible for his or her false impression about your personal life.

The information stays online forever

A photo or a comment uploaded on a social networking page is available to a number of users. Even if you choose to withdraw this information by deleting it, it still remains stored in files of the company where the page belongs to, it's just not displayed on the Internet. While you might think that you have erased any trace of it, someone could see it in the future or copy it and use it for his or her personal benefit.

Disclaimer Copyright

In several of the social networking sites, like Facebook, there is a specific term and condition that has been set up for the users during their registration, which is the renouncement of the copyright for uploaded content. As a result, images that you upload and share become the property of the company and can be used at any time from anybody.

Harassment - Stalking - Cyberbullying

When people share their personal information such as name, address, telephone number, school name, business information or company location, they make them public knowledge that can reveal their real identity. All those information that people upload without being aware of the consequences may be used against you in order to threaten you or harm you. Especially it should be noted that when you upload photos, people can manipulate and distribute them in order to disgrace you or threaten you.

Positioning

Many users choose to post on their social networking websites their location. This could happen either consciously, by choosing to share your current location through the website, or automatically, using applications on your phone. However, you must remember that by sharing your location you expose yourself to dangers because this information can turn out to be harmful for you, by letting abductors know your location or aspiring burglars when you are away from home.

Identity Theft

In this case a user of the Internet misleads or harasses other users by pretending to be you. The identity theft can be achieved in two ways: a) theft of your real profile, and/or b) creation of a new profile that includes your own details such as name or photos.

Disclosure of personal data from other users

It is essential to mention that even if you try to do your best, sometimes this is not enough. For example, you should keep an eye on things that other users may share, because they might involve you. The truth is that we cannot always control the information concerning us that others make public. For example, a friend may post on his or her profile a photograph among others, including you in an inappropriate pose, or may reveal the location you were without you being aware of that. Also, by declaring someone to be your classmate and notifying the school you are going to, you automatically reveal an address where someone can find you.

Allocation of data to third companies

The companies holding the social networking sites have access to the information you post but also to data that can be derived from your connection, such as the IP address, the geographical area and the browser you are using. This information may be granted to other companies and used in targeting you for advertising purpose.

HIDDEN RISKS IN SOCIAL MEDIA NETWORKING

Allocation of data in applications

In many social networking platforms, apart from posting information in your profile, you are able to use other applications as well. Those are not always certified for their safety and they may gain access to personal information on your profile, such as your address, or contain malware (viruses, etc.).

Specialized scams

The information you post on your profile can be used by corrupted and devious individuals to tailor their attacks (phishing) and to have a greater chance to deceive you or your friends.

TIPS FOR YOUR SAFETY

Privacy (Personal Details)

- Do not post information that could help a stranger to track you down, such as your address and phone number, the company you are working at or the school you are attending: those information can be used by strangers in order to approach you.
- Remember that your address or personal information of your neighbors or your classmates can betray you as well as your location. Do not post photos with your valid and precise address details.
- Do not use the social media as your personal calendar. Your profile does not need to contain all the information about your daily activity (what you do or with whom).
- Check for security and privacy settings for your profile. Adjust your information so that it is only visible to friends.
- Do not allow unknown applications to use your account information beyond your name, unless it is strictly necessary for the service, or do not allow them posting comments on your account.

Avoiding situations of embarrassment

- Think before you post a comment or a photo. Will the information or comment you post be seen by your family or your future employer? Can this post jeopardize your career or your intimate relations in the future?
- Before posting an information on the social media think that this information will never be erased from the Internet. Could this have a negative impact on your future life?
- Check the content posted by your friends on the social media. Does it correspond to the public image you wish to present? Remember: “Show me your friends, and I’ll tell you who you are.”
- Respect your friends’ rights and privacy. Could the information you are posting concerning your friends cause them trouble? You should first ask for their permission.

Do not trust strangers

- Do not accept friend requests from strangers. Do not trust the data their profile indicates on the social media, because the name, age and even photos of their profile may not be true.
- Pay special attention to your children. Talk to them about the dangers and the risks that the social media hide and don’t allow them to meet people with whom they came across through these applications.
- When you accept friend requests from people you know in your real life, communicate with them and verify before accepting the request.

Attempted Fraud

- If a friend contacts you asking for money, first call him or her to make sure that scammers haven’t stolen his or her profile.
- No social networking site will ever send you an e-mail asking you to confirm your password by filling a form. If you receive such an e-mail, it is probably an electronic attack (phishing).

Account Security

- Make sure that the security code you choose for your account is “strong”. Do not use passwords that can easily be guessed, such as your date of birth.
- Do not use the same password on other accounts, such as your e-mail, and remember to change your password at regular intervals.
- As with any other security code, do not reveal the security code of your profiles to third persons and do not fill in forms online, except when logging in. Remember that no social networking site will ever send you an e-mail asking you to confirm your password by filling a form.
- If you think that your account has been stolen, report it immediately to the administrator of the social networking site through the proposed process (report).
- Review the procedures for protecting the privacy of your account, check the available account security options provided by the social networking tool, and turn them on. If you choose alternative ways to recover your account or choose to restrict people who see your profile, select this option when creating your account. Visit your account settings regularly in order to discover new services offered by your social network webpage.

Terms of use

- Before you create an account at a social networking page, read carefully the terms and conditions of the security policies. These may include the condition that waives copyright for the content you post, or the right of the company to grant to third companies your personal information. If you do not agree with these terms, do not proceed to creating the account. Not skipping this step is very important.
- Re-read the terms and conditions of the Security Policy at regular intervals. When you create your account you accept that they might change without notifying you.

FACEBOOK

It is the most popular social networking site with over one billion users worldwide.

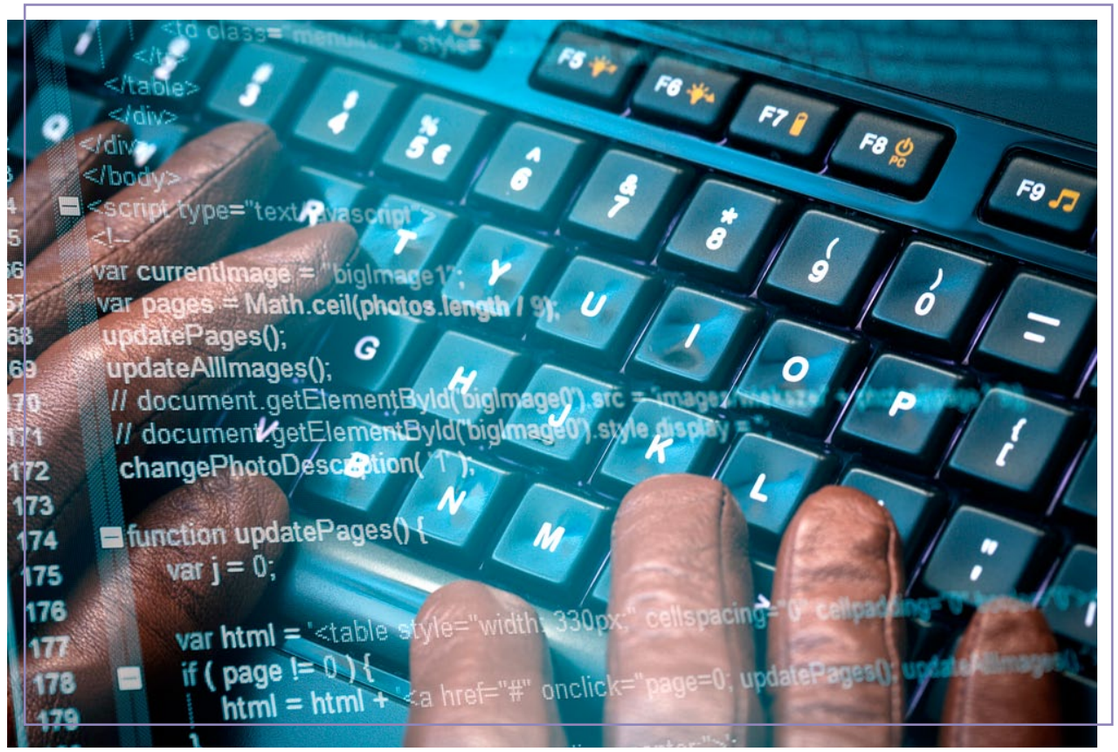
- It started in 2004 as a page dedicated to communication with friends and relatives. It became a world-class company, culminating in being listed on the New York Stock Exchange in May 2012.
- The company is located in California, USA. Although the content of the page is translated into Greek, there is no company’s representative in Greece.
- Under the terms of use of this site, you agree to the transfer and processing of your data in the USA.
- The basic services provided by the Facebook platform is the creation of a profile or chronological timeline that can been seen by each user wishing to be your friend.

USEFUL INFORMATION

- Each user can organize friends into groups and choose what information others will see. If you do not choose this option on the privacy settings of the account, then such information may be seen by everyone and become public.
- Under Facebook's terms of use, in order to become a user you should be over 13 years-old.
- Anyone who creates a Facebook profile accepts the terms and conditions of use, which raise a number of issues concerning the legal relationship with the Facebook Company. Within these is the right of the company to change the terms of use, without informing you.
- According to the Facebook terms of use each user submits his real name and personal information. In reality, there is no mechanism verifying the identity of a new user. If the company discovers that someone has stated false data, it has the right to close the profile and shut down the page.
- The Facebook Company clearly states in the terms and conditions that it cannot guarantee the security of each user's account.
- Through the Facebook platform every user can use applications from third party applications that are not within Facebook's jurisdiction. Thereby users give access to personal data to companies apart from Facebook.
- Facebook reserves the right to use the profile of a user in advertisements that appear on the page, unless you explicitly declare that you don't wish to. It also reserves the right to allocate in the future the name and photo of a user to other companies for advertising apart Facebook.
- Together with the information that someone posts on their profile, the Facebook reserves the right to collect other data for each user's account, such as the IP address of the connections and the browser that has been used. In this way, it can extract more information, such as a user's geographical location.
- Facebook collaborates with police authorities around the world, following a formal legal procedure (request of judicial assistance or in specific cases prosecution order). The reporting is based on the principles of police cooperation and the legal framework of California.

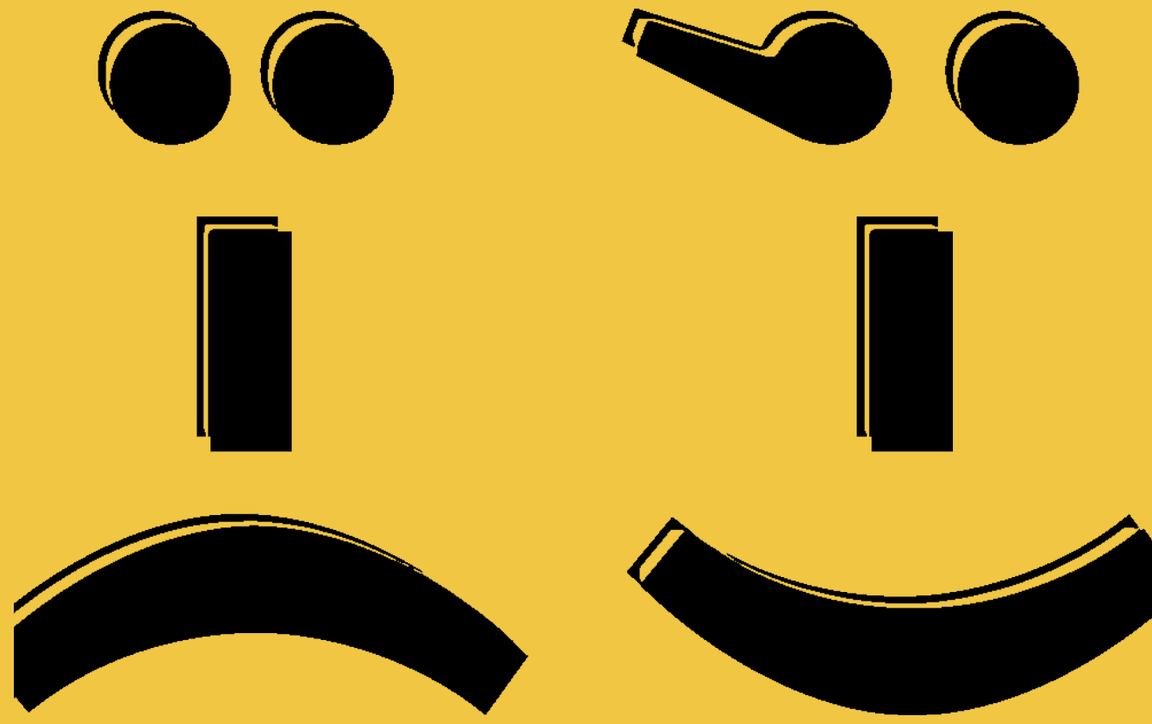
TIPS

- Read in detail the terms and conditions of use before creating an account (sign up). If you do not agree with any of these terms, do not proceed in creating the account. Revisit the terms and conditions of use at regular intervals in order to check eventual changes **(www.facebook.com/page_guidelines.php)**.
- In each comment that you post or photo you upload, choose the individuals that you want to have access to them. In order to do this there is a selection button next to "Post", that allows you to specify whether it will be public or visible only to your friends. You can also choose specific individuals or a list of people from your friends who will be able to see this post.
- Select in the account settings if you want information such as your name and profile picture to appear in ads that are placed on Facebook. Also, select whether you want Facebook to use in the future your information for advertising outside Facebook.
- Before you allow an application (App Facebook) to access your profile, you must read carefully to what information it has access and which are the actions that will be performed on your profile.
- If someone is bothering you on Facebook, report it to the administrator of the website by clicking the "Report/Block" option located in his or her profile. In the actions menu you can specify how this individual harasses you. For example, he or she might impersonate you (identity theft) and cause you problems. You can also choose to block any user who is bothering you, in order not to receive his or her messages.
- Protect the security code (password), like any other password. Do not disclose your password to third persons, as they might be use this opportunity in the future to impersonate you. If someone stole your account password, follow the procedure of the page to "lock" and recover your account (**www.facebook.com/hacked**).
- Use the help for every question you may have about the way Facebook is used and works (**www.facebook.com/help**).



child _pornography

when childrens' safety is threatened online



Some of the most frequent offenses Cyber Crime Division faced during the past few years, considering a) the development of technology in computers and mobiles, b) the evolution of the Internet by creating countless websites and apps for social networking, electronic conversation (chat), with possibility of using the camera, exchanging files, cloud, e-mail, and c) the anonymity of the Internet, are linked directly to the development of child pornography (Article 348A PK) and sexual assault (Article 337 PK) and seduction (Article 339 PK) of minors.

The Cyber Crime Division has been certified by the Interpol as an official Service when it comes to the identification of sexual abuse victims from around the world (VICTIM IDENTIFICATION via INTERPOL'S ICSE DATABASE).

The production of child pornography is a global phenomenon with massive profits.

Nowadays, all around the word the heterogeneous groups of child pornography are rising massively since child pornography is considered to be the second most lucrative criminal activity after drug trafficking. This is because child pornography produces great financial profits, while it falls under the umbrella of organized crime.

In Greece:
In recent years a rapid increase in the number of Internet users who download illegally videos and photos involving child pornography has been noted.
However, up to this day, despite some isolated cases, the existence of an organized circuit aiming at filming acts of sexual abuse to minors hasn't been established.

HOW "PREDATORS" WORK
GROOMING (SEDUCTION OF A MINOR)

Grooming is considered to be the activity of "predators" pretending to be teenagers, using open chat rooms, social networking sites and other online communication sites to attract children in order to abuse them. The victims of grooming may suffer severe traumas that have psychological and emotional impact, with severe effects on their health and well-being. The victims of grooming face various types of abuse, whose consequences and impact vary according to the victim and the way it experiences this process. The abuse that a child involved in grooming suffers is not only of a sexual nature, but also emotional, as children find it very difficult to cope with the demands and pressure of "predators".

It is noted that during the period of adolescence young people make their "personal revolution". This attitude of independence motivates young people to find new acquaintances through the Internet, rendering adolescents the most vulnerable group as far as pornography and sexual harassment are concerned.

Such websites are often perceived by children as safe chat sites on the Internet, both because of the public nature of the communication and of the incorrect perception of children who believe that their anonymity is maintained and that there is no way the other person they communicate with will find out their true identity. The "predators" begin the discussion with their potential victims in order to develop a friendly relationship with them, and gather as much information as possible about their place of residence, interests, hobbies, and sexual experiences.

The discussions can last days, weeks, even months, until the "predator" gains the child's trust. Then the "predators" slowly start to communicate in a more sexual style which involves sending pictures as something acceptable and normal. Those methods aim at undermining the reluctance of children to take part in sexual intercourse, but also at preventing the victims from seeking protection from their parents and teachers, since the victims end up feeling guilty for having exchanged this type of images in the first place.

The "predators" are usually people above suspicion, educated, with a good economical background. Usually they have their own family, they can be model fathers or characterized as respectable individuals. For example, in this category may fall scientists, teachers, businessmen, etc. **These people don't hesitate to take advantage of their social status or their relationship with their relatives in order to fulfill their needs and their passion.**

Usually "predators" have pedophilic tendencies and, if they can't have access to minor children, get involved with them and accomplish a sexual act, they tend to satisfy themselves through the Internet, wich allows them to gain access to pornographic material related to children, with one and only purpose: to fulfill their sexual needs.

HOW THE CIRCUITS WORK

These “closed groups” communicate via newsgroup, via communication rooms (chat rooms) or via e-mail. Ordinarily, the circuits that traffic pornographic material use misleading photos in the home page of the website. The websites where child pornography is uploaded are “camouflaged”, in order to be untraceable. They create videos in which they mix adult pornography with child pornography, in order to complicate their identification and tracking.

Tips for Children

- Consult your parents, when a problem occurs with someone who approached you on the Internet, via a website or application.
- If you have an account in a social networking site (after the age of thirteen), avoid submitting your personal information (name, address, phone number, or name of the school you are attending), as well as photos of you or your classmates.
- If you want to post your photos on various pages of social networks, you must be careful that they do not show your body’s sensitive parts or your face, and that they are taken from a distance.
- Use a complex and not predictable password for your account profile. Also, it would be good to notify your parents and let them know your password, for safety reasons.
- Do not accept friend requests from strangers.
- Avoid entering pages that require talking to strangers or where their username is not displayed or is required the use of a camera.
- Never open the camera to strangers.
- If someone in a conversation asks you to take a photo of your body or your face and to send it to him, don’t do it and notify your parents immediately.
- Do not open messages/e-mails and links they contain, even if a friend of yours sent them and especially when you do not know where the link leads; a virus might be contained.
- If a stranger approaches you and starts a conversation with sexual or inappropriate content, stop talking to this person and responding to his messages.
- If for any reason you experience insecurity or fear, it is advisable to notify your parents or call our Service at 11188 for help and support.
- The Internet offers a fictional reality and, therefore, does not allow you to choose your friends having a comprehensive view of who they are. It deprives direct contact with your social friends, which means that you must be very cautious about who you talk to, who you are associated with, or what you share with them.

It is important to consider that when you communicate with a person through the Internet you are not able to know what this person does at this precise moment, his motives and intensions. This means that you don’t know how he or she will be using a picture you sent, whether he or she is recording when you activate your camera.

Tips for parents

No matter how a person intending to approach your children and violate the provisions of the aforementioned Articles might operate, the following can be observed:

1. Children often ignore who they are talking to or don’t take into account the risks of talking to a stranger. Sometimes, children might think that they talk to their friends but it is possible that someone has hacked their page or violated their profiles. Usually the person who talks to your children uses an attractive and manipulative style, in order to trick them into sending personal information, such as names, addresses, phone numbers, into uploading or sending photographs with provocative content through their computer and mobile phones (Smartphones) or even into arranging a meeting face to face with them.

Subsequently, the children can become targets of cyberbullying, receiving, for example, threats or being blackmailed to send pictures of them probably with inappropriate content.

Websites and applications where these can occur are social media and online games with communication platforms (chats).

2. Children tend to privilege the Internet and the web pages as a way of spending their free time, having fun, acquiring knowledge or solving questions. They might also want to follow “fashion”, e.g. taking photographs of themselves (selfies). Such actions, as well as open links of unknown content from a website, an application or a service such as e-mail, could be a form of danger, because children ignore that those websites may display an inappropriate content for children, or contain malicious software that can be installed on computers or mobiles, leading to unexpected results for the child’s safety.

3. Taking into consideration the aforementioned risks, we inform parents on the measures that should be taken in order to keep their children safe and prevent them from exposing themselves to risky situations:

- The most important thing you should bear in mind is to establish a strong bond of trust and communication with your children: this is the only way to prevent your child from becoming a victim. However, in case of any doubts or incapability to handle the situation, you could talk to a psychologist.
- You should keep an eye on their child’s devices and their storage media, through which children enter websites, applications and services for any purpose. If you don’t have the necessary expertise, then it is advisable to seek expert advice.
- It would be helpful for both you and your children’s safety to know their child’s password for the social media web page they use, in order to have full supervision of their child’s communications.
- It is best if young children, especially under thirteen, don’t have accounts on social networking sites or, if this is not an option, it would be very helpful for children to have good communication and the proper restrictions for access by third persons, e.g. search available only to friends.
- Avoid uploading or mentioning in a discussion personal information such as names, home addresses, phone numbers or name of schools, as well as photos and e-mail addresses in the relevant websites, applications and services.
- Avoid uploading or sending photos with obscene content.
- If you upload standard photos with normal content, be sure not to show children’s faces, or that the pictures are taken from a distance, especially if your child is under thirteen years old.
- Do not accept strangers into your children’s profiles.
- The ideal would be that the friends that your children have in social media profiles are the ones that they have in real life.
- Avoid entering pages that use electronic conversation applications (chat) unknown to children and where it is possible to chat with strangers, as well as to use a camera to communicate with them.
- Avoid opening any link from unknown origin and source.
- We advise children to avoid camera use, especially when their conversation is going to be with strangers or without the parents’ presence.

An essential reminder to all parents is that you shouldn’t upload pictures of your children in your own social network profile. This way you protect both yourselves and your family, since it is best that the moments you usually captivate through a photo remain personal.

In case parents identify a problem:

- We talk with the child to fully investigate and understand the scale of the problem, its source and the possible damage that has been done. Make clear if the child is involved only through conversation, if he/she has sent photos, what kind, how many and to whom, or if the camera has been used and through which application.
- You could also consult a psychologist in case you fail to communicate with your children for any reason or if you face difficulties in managing his or her behavior.

For the collection of evidence, before any exclusion (block) or communication through deletion (including chat and photos) with the stranger, for any other instruction or help referring to the legal part of the problem, you can call our Office at 11188.

HOW THE CIRCUITS WORK

Some of the international operations where our Service participated:

- **CAROUSELL I & II**
- **KOALA**
- **STORM**
- **PURITY**
- **MYOSIS**
- **TWINS**
- **CHARLY**
- **SPIDER WEB**
- **ICARUS**
- **ANGELS**
- **Hydra** (During the operation 78 users-perpetrators from 32 different countries were identified by the Department of Electronic Crime.)
- **Depletion**
- **Depletion 2**
- **Sornyak**
- **Rina**
- Chat scanning [Scan of online virtual communication rooms (chatrooms)], during which investigators using profiles-accounts in electronic conversations impersonated minors under thirteen years old.

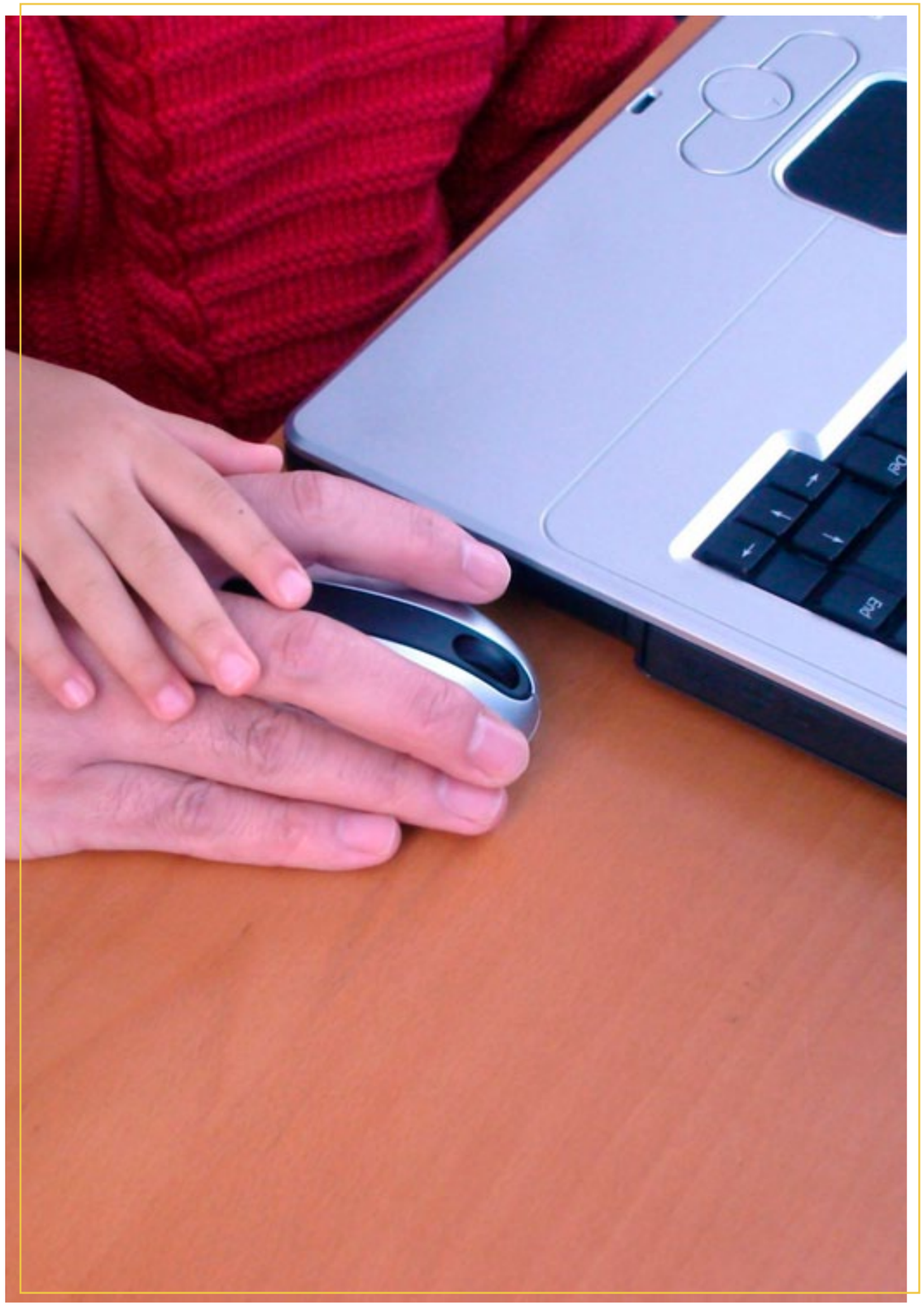
Also, the "Pedophilic Communication Code" was published online for information and sensitization of parents.

The "Communication Code" stems from a manual discovered in the Dark Web, after several months of research and targeted investigations by specialized Electronic Crime Officers.

The material of child pornography involving minors and children is disgusting and horrifying. From **a few months old infants to 17 year-old adolescents**, children are the tragic protagonists of those sick and inhuman sex videos and photos involving minors that under the effect of drugs are forced to have a sexual intercourse between them, with adults or even with animals.

Most photos and videos come from countries in Latin America, Southeast Asia and Africa, such as Venezuela, Brazil, Thailand, Singapore, and Algeria.

The cost for the acquisition of photographs and videos varies according to the protagonists' age or their contents.



industrial _espionage

when every company is electronically assaulted

THE FUNDAMENTAL DECALOGUE FOR YOUR BUSINESS

Antivirus - Antimalware
You should have an antivirus program and a protection against malicious software (Antimalware), which should be informed on all current threats.

Firewall
By using the firewall, you can track and locate any unusual actions of a specific program. The firewall is the heart of security policy because it filters and observes any move of your company's network.

Intrusion Prevention System
The Intrusion Prevention System looks for viruses and monitors your systems for any unusual activity.

Users
User access policy to the company network.
Control user access to the company network via:
Authentication: Authentication of users – Confirmation of user identity.
Authorization: Determination of permitted actions for each user.
Accounting: Create action files for each user (what actions he or she did and when).

Remote access users. Any user will be linked to your network via a suitable Virtual Private Network (VPN) followed by the security levels.

Train users, so that all users understand the importance of the faithful implementation of security standards. Some indicative safety rules may be: to turn off the computer before leaving the office and use strong passwords. Moreover, the system should not allow a user to access the network if strong password is not used.

Audit of software licenses. Users will not be allowed to download any software of their will because it can endanger your business network.

Apply access policy for users and the enterprise's printed material.

Apply sanctions to any user not implementing the company's safety policy.

Security policy concerning the devices used
Configure critical devices not to support the use of portable data devices, e.g. USB.

Do not allow people outside the company or visitors to connect to your company network.

Use Software Data Loss Prevention (DLP) to prevent critical business data leakage.

Restrict access area
There should be safeguards so that, if an attacker manages to enter any part of your network, he or she cannot automatically have access to the entire network.

Know the weaknesses of your network
There is no perfect security system, so the operator should know the vulnerabilities and areas of greatest risk, be able to prohibit access to them, and make sure that your company is safe.

Patent Ensured
Safeguard the business-critical data with patents wherever possible.

Monitor the natural environment of your business using security cameras

Estimated costs
Pay particular attention to security cost estimation and include it in the company's budget, since it is crucial for its existence.

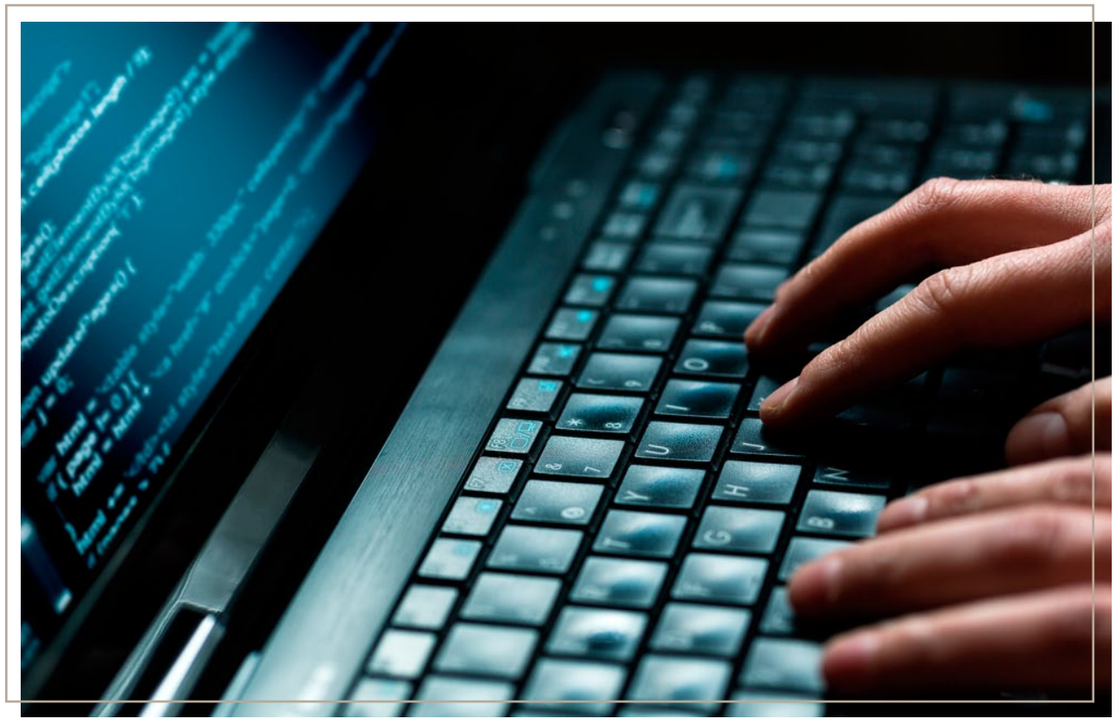
If you fall victim to industrial espionage inform directly our Division by phone at 11188, or via e-mail at **ccu@cybercrimeunit.gov.gr**

Definition

By the term industrial espionage, we refer to a company collecting valuable data from other companies or by its private hackers in order to improve its comparative advantages.

Internet_fraud

Financial Crime



The basic principle of Internet fraud is to convince the victim to pay a small initial amount in order to secure a much larger in the future, as in the case of the Nigerian scam, or persuade the victim to the safety of online transactions in order to extort large sums of money (credit card fraud, etc.).

SPAMMING-SCAMMING

The word “spam” describes the massive sending of messages through computer (e-mails), which usually have an unprovoked and commercial nature, and are send indiscriminately. When the sender’s basic goal is to trick the victim and to use maliciously the data he or she will intercept, then the process is called “scamming”. This is the most common mode of action in many kinds of electronic financial crimes (Nigerian scams, Spanish lottery, phishing, fraudulent jobs abroad, ads for weight loss, etc.).The massive sending of malicious messages can also attack a mobile device, since nowadays the use of Smartphones is growing rapidly.

NIGERIAN SCAMS

This method is based on an e-mail which informs us that someone (usually a former senior executive of the Nigerian government) needs our help to convey a big amount of money (e.g. 30 million dollars), which cannot be channeled out of the country under the name of the account holder/e-mail sender. Promising a high fee (a percentage of the capital), the sender requests that the e-mail recipient helps by receiving the said amount. The victim is informed that he or she was not chosen randomly, but on the basis of information concerning his or her solvency (often a chamber or professional association is mentioned). At the same time, the offenders stress particularly the issues of confidentiality and trust that the victim should be respected. When this aim is achieved, they ask the victim’s consent and bank account information, or any other information necessary for carrying out the transactions. Quite often and on the victim’s demand, the offenders produce documents that seem authentic, in order to eliminate any possible doubt of the victim. If the victim responds, an endless process of e-mails, phone calls and letters exchange begins, making him or her think that he or she is very close to obtaining that sum of money. But, just before the final money transfer occurs, the official invokes a temporary problem (e.g. special tax, unpredictable end, an intermediate payment of staff, etc.). The official of course pretends to be unable to pay for the sum, claiming that he already has proceeded to the money transfer and that therefore the money is bound. As part of the collaboration, the victim is asked to pay the amount, which will be refunded upon completion of the transaction.

Of course this is only the beginning of a series of “problems” that the offenders invoke in order to divert money that can reach up to €500,000. Experience has shown that some of the victims are persuaded to travel to Nigeria to complete the transaction and, while the offenders have reassured them that no visa is required, the victims end up being illegally in the country, and exposing themselves to blackmail by the circuit of offenders.
In some cases, the victims were convinced by the circuit of perpetrators to travel abroad, and ledded to a bank where they were shown the money deposit, while they had already paid a sum for the capital to be released. They stayed at 5-star hotels and were encouraged by the circuit of offenders to spend 4 days leading a luxury lifestyle, that the offenders pretended to pay for, without intending to do so.

SPANISH LOTTO

This form of fraud is carried out by sending bulk e-mails to random Internet users. These messages inform the users that they won a large sum of millions of dollars through an electronic draw on the Internet, where they have never taken part. In order to be credible, the perpetrators use names similar to those of large companies (e.g. Microsoft, Yahoo etc.) and they accompany their messages with false certificates referring to the supposed electronic draw. The scam occurs when the perpetrators ask the supposed winners to prepay some taxes and/or the costs of disbursement for the money – usually an amount of a few thousand dollars.

PHISING PERSONAL INFORMATION

Phishing is usually performed by sending bulk spam e-mails, purportedly from a real and legitimate company (bank, online store, online payment service etc.). The aim of those e-mails is to deceive the recipient and steal confidential personal and financial data. Then the fraudsters use these data to perform financial crimes. Concretely, the sender requires the recipient to update or to directly verify some personal information for security reasons, which in the end leads through links to phony websites mimicking the official. The worldwide annual earnings of the offenders exceed 1 billion euros.

PHARMING

Pharming is a process similar to phishing. This process consists in the intervention of third persons in a website's DNS server, aiming to redirect the browser to other false websites. The pharming can occur by altering:

- the "host" file of a PC, thus redirecting the domain name to a false destination,
- the "router" of a LAN network: by altering the settings or even the firmware of a router, the perpetrator can redirect a domain name for all PC networks,
- one DNS server: the attackers gain access to a central DNS server by altering the movement of all Internet users served by them.

In other words, when an Internet user enters an online store website, he or she is transferred without his or her knowing to a fake website, which simulates the actual store site in order to mislead and defraud the user. Then the perpetrator takes hold of personal information that the unsuspecting user has submitted during the transaction process (name, credit card numbers, etc.) in order to use them in a malicious way.
Pharming has recently occurred into two banking institutions. When using the web-banking services through a contaminated PC, the users were redirected to false websites where the perpetrators stole their personal information.

CREDIT CARD FRAUD

Fraud cases involving credit card use for online shopping are constantly growing. It is estimated that banks suffer losses of millions because of individuals manufacturing, counterfeiting, stealing credit card numbers, or making virtual purchases via Internet using card numbers that are relatively easy to obtain or generate through algorithmic programs. Moreover, the absence of face-to-face communication in the Internet makes the perpetrators bolder. Products purchased online and never delivered, excessive credit card charges for services never requested or initially presented as free, misleading information on products purchased online: these are some of the citizens' complaints received daily by law enforcement authorities in Greece.

For example, people interested in purchasing a car, a tractor or a machine, tend to search online ads that meet their needs. Once communication with the owner-offender is established, the victims pay a deposit, usually through payment companies (e.g. Western Union). After that problems occur since the offenders put forward various excuses to collect extra money, to postpone and finally avoid product delivery.

Pyramid Scheme

Among Internet frauds, there is also the online pyramid scheme of work at home. These scams promise high wages and abnormally high profits from investments which do not actually exist. Eventually, the system collapses as investors are not paid nor the promised shares neither the agreed return, losing thus their initial investment.

Jobs

The global economic situation has brought forward another type of fraud: deceptive online advertisements posted on job sites or sent to the victim via e-mail that describe particularly attractive jobs, usually abroad. Perpetrators do not hesitate to create the company-employer's website, where they post information on deceptive ads to be even more convincing. Then they ask unsuspecting prospective employees to disclose their personal information, even upload copies of their personal documents such as driver's license, identity card and any other detail considered "useful" and "required" for their job. Subsequently, the candidate is informed that, since the employing company does not hold a bank account in his or her country, one of the company's creditors will grant him or her a check for expenses and salary. The check usually exceeds by large the agreed sum and the applicant is asked to transfer the surplus to the employer. After the process is completed, the candidate realizes that the check is counterfeit. In other cases, the victim is persuaded to pay a fee to make sure he gets the fake job.

DEBT ELIMINATION

The current economic situation has led to another flourishing kind of fraud: websites promising the management and elimination of household and business debts, advertising legitimate ways to pay off mortgages and credit cards' debts. Usually, all that is required is to pay an initial sum, to send all necessary information concerning the loans or credit cards, and of course to give authorization to the person who will carry out the process. The mediator then issues bonds and notes to the lenders who aspire to the payment of all legitimate debts. In return, the victim is required to pay a percentage of the debt's value to be covered by the mediator. The aforementioned process is particularly linked to crimes related to identity theft, as participants provide all their personal information to the mediators.

BOTNETS

Millions of computers have become, unbeknownst to their users, subservient to organized hackers threatening the overall functioning of the Internet. Up to a quarter of computers connected to the Internet are infected with hidden software that implicates them to malicious networks, known as botnets, according to the "Internet's father", Vid Surf (inventor of the TCP/IP protocol). The phenomenon seems to gain the proportions of an epidemic, since about one in six computers with Internet connection have turned into botnets' "zombies".

A computer is considered a "zombie" when it is connected to the Internet and controlled by an external user. This external user is usually a hacker who, having unleashed a successful attack against

BOTNETS

the computer, has managed to turn it into a "zombie" computer. This attack includes infecting the victim's computer with a virus or Trojan horse. The "zombie" computers are mainly used to send unwanted or malicious e-mails (spam-scam). In this way, spammers can avoid detection and use the "zombie" computer's owner bandwidth (bandwidth) for their own purposes. These botnets are used to perform DDoS attacks, brute force attacks on information systems and during pharming frauds by constantly creating fraudulent clones at different sites around the world. The largest botnets on record so farnumbered up to 30,000,000 PCs!
In Greece, a large industrial organization fell victim to a botnet that intercepted all electronic conversations after attacking the mail server using a botnet. Also, a banking organization received a severe blow when users of the bank's online services fell victims of fraud, their H/PCs becoming "zombies" due to a special "Trojan" program.

VIRUS RANSOMWARE

Another example of a phishing method is the ransomware virus or, as it is now known, the "€100 virus". The attackers exploit weaknesses of the victim's computer to infect it with malware as he or she browses the Internet. This software "locks" all PC functions and displays on the monitor a message supposedly by the Electronic Crime Division informing the user that he or she got €100 fine for having allegedly violated the Criminal Code. The payment of the fine may be performed using prepaid cards or pay safe cash. This is a virus with a pan-European presence, using the police force's emblems of the country from which the victim's PC has access to the Internet. Thousands of users have fallen victim to this fraud and a certain number has ultimately paid the disputed amount. This is a perfectly organized circuit through a complex process and through mechanisms of repaying black money, manage to break prepaid cards €100 to €10 value cards which and distribute worldwide.

CELL PHONES AND INTERNET TRAPS

The use of mobile phones and of Smartphones in particular is growing rapidly over the last decades, and more and more users need them as essential tools for their everyday lives. Cybercriminals take advantage of this evolution and cause frauds costing several million euros by the sale and purchase of software applications for mobile phones, such as the localization of the mobile phone of a loved one. Usually the unsuspecting user is asked to enter his mobile phone in order to obtain the chosen application. Then, the mobile phone number is charged exorbitant sums, according to the small print in the terms of use that the majority of consumers do not read.
A type of fraud that is particularly common in foreign countries concerns online auctions. Such scams focus mainly on distorted presentation or non-delivery of auction products. Consumers should be especially cautious when sellers ask them to pay the agreed amount to the account of a third person, or invoke exceptional reasons that cause them to leave their country, or when the sellers ask them to make the payment through Western Union or MoneyGram.

LAWS IN PRACTICE

In order to address the delinquent acts taking place over the Internet and to constitute the offense of "fraud", the Electronic Crime Subdivision executives are and guided by two key articles of the Greek Penal Code (PC): a) Article 386 "Fraud", and b) Article 386A "Computer Fraud", described briefly as follows:

Article 386 "Fraud"

1. Whoever, in order to gain for himself or others an unjust profit, damages foreign property, persuades someone to act, omits or tolerates knowingly representing as true false facts or unlawfully disclosing or concealing true facts, shall be punished with imprisonment of at least three months and, if the damage caused is particularly large, with imprisonment of at least two years.
3. An imprisonment up to ten years is required: a) if the offender commits fraud by profession or habit, and the total benefit or total loss exceeds the amount of fifteen thousand (15,000) euros, or b) if the total property benefit or the damage caused exceeds the amount of three hundred thousand (300,000) euros.

Article 386A "Computer Fraud"

Whoever, in order to procure for himself or others an unjust profit, damages foreign property, by affecting the computer components through incorrect configuration of the program, intervention in its application, use of incorrect or incomplete information or by any other way, is punishable under Article 386. An asset impairment exists even if the person prejudiced is unknown. It is irrelevant whether victims are one or more persons in assessing the damage amount.

HOW MUCH DOES CYBERCRIME COST IN BUSINESS?

One of the world's largest technology companies presented at the end of 2012 a survey, which shows that the cost and frequency of cybercrime continue to grow for the last three consecutive years. According to the third annual survey involving multinational companies in the US, the incidence of cyberattacks has sharply increased within three years, whereas the financial impact has increased by about 40%. The research for the cost of cybercrime for 2012 (Cost of Cyber Crime Study 2012), conducted by the **"Ponemon Institute"**, **showed that the average annual cost of cybercrime** on an indicative sample of firms in the US amounted to **$ 8.9 million**. This figure shows an increase of 6% compared to the average cost in 2011 and 38% compared to the corresponding figure for 2010. Furthermore, this year's survey shows a 42% increase in the number of cyberattacks, with organizations facing an average of 102 completed attacks per week while facing 72 and 50 attacks per week in 2011 and 2010 respectively. A senior official of the company that conducted the research said:

Organizations are constantly spending more time, money and energy to respond to cyber threats, which reach levels that will soon become unsustainable. There is evidence that clearly show that the use of advanced "security intelligence" solutions "helps to substantially reduce the cost, frequency and impact of these attacks."

This year also, **the biggest cost** for businesses originated from cybercrime such as the use of malicious code, denial of service attacks, use of stolen or hacked devices, and malicious activity of persons within an organization. **Combined, the costs** resulting from these threats represent **more than 78% of the annual cost of cybercrime per organization**.

The survey also concluded the following **key findings**:

- The theft of information and the stoppage of work still correspond to higher external costs for businesses. On an annual basis, **information theft is equivalent to 44% of total external costs**, 4% more compared to 2011. Work interruption or productivity reduction accounts for 30% of external costs, 1% more compared to 2011.

HOW MUCH DOES CYBERCRIME COST IN BUSINESS?

- **The use of advanced information and incident management security solutions (Security Information & Event Management -SIEM)** may reduce the effects of cyber threats. Organizations that have used such solutions have saved about $ 1.6 million per year. For these organizations, the cost of systems recovery, threat detection and reduction was significantly lower compared to the costs facing those who did not use SIEM solutions.
- The cyberattacks may be expensive if not managed quickly. **The average response time against a cyberattack is 24 days**, but can reach up to 50, according to this year's study. The average cost for the 24-days period amounted to $ 591.780, 42% higher than the estimated average cost of $ 415.748 for the same period last year.
- The data recovery and threats identification remain the most costly internal activities in relation to cybercrime. On an annual basis, these activities account **for almost half of total internal costs**, most of them consisting in operational and labor costs.

The President and founder of the Ponemon Institute, **Dr Larry Ponemon**, said that this research aims to quantify the economic impacts of cyberattacks and to document the trends over time regarding the costs involved. He added that a better understanding of cybercrime's cost would help organizations to determine appropriate investment and resources needed to mitigate the devastating consequences of an attack.

Similar studies on the cost of cybercrime have been conducted in Australia, Germany, Japan and the United Kingdom, with similar results.

For example, the information systems security solutions company RSA published a research on the increased costs caused by phishing to UK, Canada and USA companies in the 1st half of 2012. Phishing exists for the past 16 years and remains one of the biggest dangers of the Internet. The costs increased by 19% compared to those in the 1st half of 2011, which caused a $ 687 million loss for the American companies. The research showed that the UK, the USA, Canada, Brazil and South Africa are among the countries where most phishing attacks occur internationally. In Canada specifically phishing apparently increased by 400% during the first half of 2012 compared to the corresponding period of the previous year, which may be due to the country's economic stability and the rate of almost 1:1 to the US dollar, as "scammers" like to follow the money. In any case, despite the fact that phishing already counts 16 years of life and is considered an "old" phenomenon, no one can ignore a damage of $ 687 million.

ONLINE TRANSACTIONS SECURITY

Over time, more and more companies are active on the Internet, increasing their revenues, reducing costs and facilitating users. In this way everyone can have 24-hour access to the company's catalog and buy whatever he or she needs. Most websites selling products use payment-transaction systems, such as Paypal, interbank systems, etc.

But are online transactions secure and safe?
How can we be sure that we will not be victims of fraud and how we can detect fraud in order to avoid it?

WHAT SHOULD YOU DO TO PROTECT YOUR TRANSACTIONS?

1) Do not make transactions using **public computers** (from net cafés, coffee shops, libraries, etc.). They may have key loggers or spywares, unbeknownst to the staff. So, malicious users can easily steal personal data and effectuate transactions in your place.
2) When you use the computer to make a transaction you should be sure that all **necessary security measures recently updated** (firewall, antivirus, antispyware, etc.) have been taken.
3) When you compare products from different websites, you may find in some of them **the same products cheaper than in other websites**. It would be advisable, then, to check whether these websites are "ghosts" (a Google search with the name of the cheap products website suffices).
4) Always make your transactions by **typing yourself the web page address**. Do not click on e-mail links, as they may be deceiving.
5) Make your payments-transactions only through websites that bear the **security icon** (a lock on the left browser). This icon is particularly important, when you type a card number or any other personal information and click on send.
6) Verify that when you type your personal information or details, the browser indicates **https** and NOT http.
7) Before you make a transaction via a website, **you should call** the online store in order to verify whether it exists. If there is no reply, it is most likely that the purchased product will not be sent, even if it has been paid for.
8) Always keep in your computer or print receipts of purchases.
9) Be extremely careful about transactions via **money transfer companies and international payments** (Western Union, MoneyGram, BidPay, etc.).
10) Be sure that the codes, debit-credit cards numbers and other sensitive information **are sufficiently secured** so that no one can intercept or memorize them.
11) Be sure to **change** your **passwords** at regular intervals, and that they consist of small and capital letters, numbers and symbols.

WHAT SHOULD YOU DO TO PROTECT YOUR PURCHASES?

1) Never prepay a seller you do not know, even if he or she reveals his personal details or his or her bank account number.
2) Seek information-posts on how the online store manages any customers' complaints.
3) Request the original receipt or written proof of purchase.
4) Pay particular attention when the offer seems too good to be true and when the seller continually pressures you for the completion of the sale.
5) Be careful when asked to pay large amounts to people you do not know: the transaction should be carried out in a shop or public place.
6) Be careful when purchasing a branded product that it is indeed authentic.

HOW TO PROTECT YOUR TRANSACTIONS VIA MOBILE PHONE?

1) Keep your mobile phone protection software updated and all the devices connected to it protected from malicious attacks and viruses.
2) Use a strong password in order to lock your phone device.
3) Carefully read the details of the applications you want to install before doing so.
4) Give your mobile phone number only to people you trust, and do not give others' mobile phone numbers without their consent.
5) Enable location-based service on your mobile phose in case you lose it.
6) Be careful when connecting to a Wi-Fi Hotspot network through your mobile phone.
7) Do not reply to messages whose sender you do not know.
8) Using CALLER ID to block users whose number and e-mail you do not know.
9) Have people who are trying to take photos or videos of you to first request your permission.

CAN ENTERPRISES FACE THE CYBER THREAT AND HOW?

Apart from installing system protection and security software, businesses should also train their staff and develop a "Culture of Security". Quite often, when hiring employees, a company asks them to sign security requirements and policies that they should comply with, in order to protect both the company's customer base and data. In doing so, a company should implement certain measures, which are summarized as follows:

1) Identify which data are exposed to greater risk, when the IT systems have access to the Internet (e.g. customer data or accounting and financial data).
2) Install in every PC special software (e.g. anti-virus programs, anti-spyware programs, firewalls) and change access and transaction passwords every 60 or 70 days.
3) Install programs backing up all important data (e.g. in an external hard disk) and upgrade them at regular intervals, so that there is no data loss in case of natural disaster or cyber attacks. Encrypt all sensitive and crucial data.
4) Prepare a contingency plan or alternative actions against cyberattacks, which should be checked annually.
5) Educate staff on the impact on everyone of an eventual cyberattack and more precisely of a fraud. The training can include seminars on Internet practices or technology solutions convincing employees that they should be particularly vigilant against online scams, as they may be duped and harmed in their personal lives through the Internet.
6) Sign contracts with the employees binding them to report to the competent authorities any suspicion or realization of an online fraudulent transaction.

Mini tips

1) Work only with companies that you know or whose information is immediately accessible through official databases.
2) Understand all the details concerning the services or products offered.
3) Carefully check every invoice and account you are asked to pay.
4) Safeguard your financial and banking data, and do not disclose them to unknown third persons.
5) Make your staff responsible for any wrongdoing, after they have been trained on the matter.

Tips for auctions

- Before you make an offer, contact the seller and clarify disputed points concerning the product.
- Be especially attentive to counterparties abroad.
- Check the return policies, warranty, and transport costs of the product.
- Secure the products during their transportation.

Tips for credit card fraud

- Verify that the website where you provide your credit card information is safe and known to the public.
- Verify the store displayed through the website.
- Check frequently your credit card movements through your bank or via web-banking.

Tips for debt elimination

- Check if the name, address and telephone number of the company or person considered a "savior" exist.
- Check the terms and conditions of the agreement before signing.
- Beware of companies offering only mailboxes for communication.
- Beware when a promise seems too good to be true.
- Beware when the revenue or profits promised are too high.
- Beware if you are prompted to prepay money on procedural matters.
- Beware of job offers that do not require experience as an essential qualification.
- Verify that the company-employer is real.

Tips for Nigerian letters

- Beware when a promise is too good to be true.
- Do not reply to an e-mail asking for your bank details.
- Do not be deceived by people posing as government officials of a foreign country.
- Be careful when you are asked to help in putting money into offshore accounts.
- Do not trust people promising large sums of money for your cooperation.

Tips for phishing

- Be suspicious when you are asked via isolated e-mail for your personal information.
- Do not fill out personal information forms sent from unknown e-mail addresses.
- Enter the website address in the browser and avoid following links.

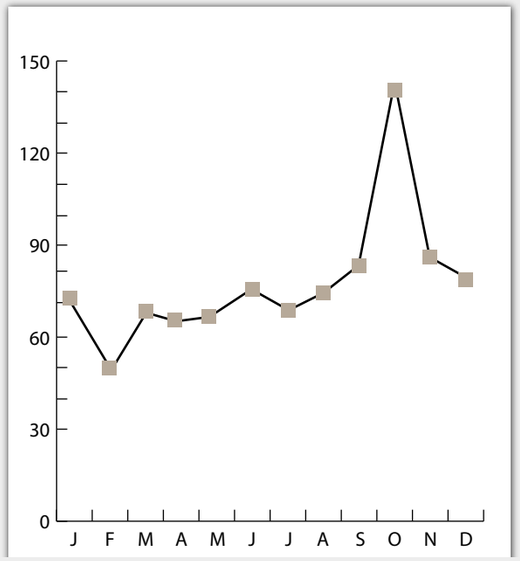
Tips for spamming

- Do not open spam messages.
- Do not reply to spam messages so that the sender does not realize that your address is real and active.
- Keep two e-mail addresses, one for your family and one for any other purpose.
- Never buy something that has been sent to you through an isolated e-mail.

In sum, you should not be afraid before making online payments and transactions. **Everyone** should enjoy the advantages provided by this type of transactions and make cheaper, easier and more varied purchases. Our Service welcomes online commerce, as long as you have and are able to handle the golden tools for all types of transactions. What are these?
a) A **prepaid card** issued by a reputable financial institution.
b) A **Paypal** account linked to a withdrawal card.
c) **E-banking** for direct access to account and card statements, but also for direct payments.

FRAUDS (MONTHLY EVOLUTION)

FRAUDS (Monthly evolution)



BIBLIOGRAPHY

http://www.ic3.gov
http://www.fraud.org
http://www.staysafeonline.org
http://www.rsa.com
http://www.businessweek.com
http://www.acfe.gr
http://www.interpol.int

EMMANOUIL SFAKIANAKIS,
KONSTANTINOS SIOMOS,
GEORGIOS FLOROS,
INTERNET ADDICTION
AND OTHER HIGH RISK INTERNET
BEHAVIORS,
LIVANIS PUBLICATIONS 2012.

ANASTASIA K. MALLEROU,
LAW OF ELECTRONIC MONEY,
LAW LIBRARY 2007.

THEODOROS N. KRITHARAS,
CRIMINAL CODE AND INTERNET,
LAW LIBRARY 2009.

CONTACT
Cyber Crime Division
Alexandras Av. 173, Ampelokipi, Athens,
P.C. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Tel.: 11188, Fax: 2106476462

Find us at:
www.cyberkid.gr
www.facebook.com/cyberkid.gov.gr
www.cyberalert.gr
www.facebook.com/CyberAlertGR
twitter.com/cyberalertgr