Newsletter - *Calibrated for Creative Communications*

Vol. 15, no. 1, Spring 2017

Spring your Garden

We are pleased to publish the Spring issue of our Newsletter with leading contributions from

- *Prof. Kálmán Kovács*, Director of the Federated Innovation Knowledge Center of Budapest University of Technology and Economics, and
- *Prof. Claudio Cilli*, Department of Computer Science, University of Rome "La Sapienza".

They will keep you focused on

- **Smart Cities**
- **Identity Theft** and the basic rules to feel more secure

You will find interest in the **ICT Development Index 2016**, not least so as to see how your country is faring along with 174 other economies worldwide.

Within the MultiCulti column, *Dorothy Hayden* will take you to **Grado** on the northern Adriatic coast.

There is more, which makes it worthwhile to dive into our Spring garden.

Take the Journey!

Plamen Nedkov

Contents

Editor

P. Nedkov, Halsriegelstraße 55
A-2500 Baden, Austria
e-mail: **info@starbus.org**, web-site: **nl.starbus.org**

The Master At Work

Partner Publication

http://mondodigitale.aicanet.net/ultimo/index.xml ■

EDITORIAL POLICY

This Newsletter maintains a world-class standard in providing researched material on ICT and Information Society activities from the perspective of Central, Eastern and Southern Europe (CESE) within a global context. It facilitates the information and communication flow within the region and internationally by supporting a recognized platform and networking media and thus enhancing the visibility and activities of the IT STAR Association.

The stakeholders whose interests this newspaper is addressing are

- IT STAR member societies and members
- ICT professionals, practitioners and institutions across the broad range of activities related to ICTs in government, business, academia and the public sector in general
- International organizations

Special arrangements for the production and circula-tion of the Newsletter could be negotiated.

The newsletter is circulated to leading CESE ICT societies and professionals, as well as to other societies and IT professionals internationally. Everyone interested in CESE developments and working in the ICT field is welcome to contribute with original material. Proposals for articles and material for the Newsletter should be sent two months before the publication date to info@starbus.org.

Smart City Solutions for Small Cities

Kálmán Kovács

Prof. ***Kálmán Kovács*** *is Director of the Federated Innovation Knowledge Center of Budapest University of Technology and Economics. He served as Hungarian minister for IT during the period 2002 – 2005.*

Together with service providers and local authorities, the Federated Innovation and Knowledge Center of the Budapest University of Technology and Economics (BME EIT) completed a targeted national research on the Smart City capabilities of municipalities. Based on our (BME EIT) survey, we decided to consider and research small-town smart city solutions to highlight the services that are suggested to be implement for certain small towns. The solutions offered from a wide variety on the palette are selected in cooperation with the local government and based on our small-town research. Short description of the collection of our Smart Small-City solutions follows.

ENVIRONMENTAL PROTECTION

Working on intelligent solutions for "risk reduction" of urban polluted industrial sites, our objective is to clean (remediate) areas with environmentally friendly biotechnologies, to increase the efficiency of remediation based on biodegradation by using environmentally friendly additives. Instead of soil replacement, we develop and apply innovative cost-efficient biotechnologies that maintain soil quality in the long run. The groundwork and application of a soil treatment technology that serves both carbon emission and holding organic carbon in the soil, and the improvement of degraded and contaminated soil.

Another topic is the "risk-free utilization" of waste for soil improvement and creation of growing medium to increase the urban green. The objective is to cost-effectively utilize industrial and household waste, to create products instead of placing them in landfills. Working out innovative technological solutions to utilize organic and inorganic, non-hazardous waste, by-products to create growing media. With growing media, we plan to increase urban green, create green rooftops for better air quality and less CO_2 emission.

CLIMATE CHANGE

A priority for cities with any size is the smart management of climatic extremes in urban environment. Urban build-up - e.g. with heat island effect - increases the effects of climate change. Heat waves are getting warmer, which demands increasing the cooling capacity of residential and office buildings. Sustainability principles must be enforced at the various planning levels – development, regulation, strategy, building and environment planning.

This includes the enforcement of pedestrian and community transport priority, in pursuit of a car-independent way of life; decrease the necessity for mobility, support for bicycle transport; development of green space system; the use of renewable energy; cycling in water usage.

Another topic is "urban air quality". The variation in the frequency and intensity of extremities (e.g. increase of the duration and severity of winter and summer smog situations) related to climate change is detectable here, as well. The sustainability planning and measures listed above - especially in the areas of transport and energy efficiency - facilitate the improvement of urban air and quality of life.

COMMUNITY PARTICIPATION IN URBAN DEVELOPMENT

Smart, built-up city and technologies cannot exist without the people living in it and using these technologies, social communities, that is, the city. Therefore, in the 'smart communities' subsystem, urban people, communities, municipalities and community institutions upholding these get the focus. It is not enough to energy efficiently renovate and equip with the latest devices a panel house or school. If the individual and the communities are not 'future-conscious', their behavior changes slowly, the individual interest conflicts with the community interest, or the economic, legal environment is not encouraging.

In our R&D activity urban groups, social strata would play prioritized roles that have EU (or global) problems, as aging city dwellers, many with 'low energy level'. How and with what societal-economic tools could this be redressed?

ENERGETICS

Several small-area microgrid ("Smart Microgrid") pilot projects are underway in different size European cities. Suggested elements of smart energy efficient grids are: city level coordination of electrical power distribution management; involving heat pumps in electric power system control; connecting energy transport infrastructures for energy storage; and developing smart public lightning system.

While furthering part of the solutions for the above elements in pilot projects to physical implementation, local endowments should be observed, and additional benefits should be exploited. These include heating of public institutions and farms, establishing biogas plants, charging accumulators of electric public transport. Collecting measurement and status data from operating and future pilots to a common platform, these autonomous microgrids could be jointly controlled, which would make the validation of computerized simulations and the microgrid – smart grid transition feasible.

One of our most promising projects is an Online Building Energetics Decision Making System with Building Typology (Smart Building as Microgrids). This includes: remote measurement and monitoring of heat and electric power consumption of a building portfolio, error reports and analyses; creation and optimization of intervention options for energy supply systems; development of building energetics smart online software for building reconstruction and small-scale utilization of renewable energy.

QUALITY OF LIFE - HEALTHCARE

The aim here is to apply technologies to improve quality of life of the elderly, to enhance their sense of security in their own homes, so they would not at all or would only later get into care institutions. With remote patient monitoring systems, a large part of hospital rehabilitation processes can be performed in controlled environments in our own homes. Another benefit is that by monitoring physiological parameters, behavior patterns and mental abilities diseases can be detected sooner and cured more easily.

Such systems are quite multidisciplinary, combine solutions from varied areas. BME EIT Healthcare Technologies Knowledge Center has close-to-prototype solutions for 'smart city' solutions:

- Development of human motion recognition, tracking and analysis programs (e.g. control the rehabilitation physical exercises performed at home).
- Use of a communication tool implementing virtual being together (replicating presence): persons distant from each other can perform various activities together.
- Monitoring physiological parameters. Based on passive sensor information, detecting and monitoring home activities.
- Application of serious games. The change in mental abilities of players can be monitored based on information from our web-based games.

INTELLIGENT TRANSPORT

Possible elements of an intelligent transport system: smart micro car renting system: just as with bicycles, with several docking points in the city. Smart car sharing software: collects destinations, and organizes traffic on the principle of car sharing, decreasing the number of vehicles in traffic and pollutant emission. Analysis of the introduction of e-car systems (charger station locations, number of chargers, the possible amount in pollutant decrease).

Dynamic traffic control, information exchange of the transport branches, optimizing peaks to prevent and minimize traffic congestion are highly suggested smart city solutions for small cities, as well.

WATER QUALITY AND WATER MANAGEMENT

The core concept of existing urban water infrastructure has been proved wrong by today: the system is not sustainable, cost and energy effectiveness is not observed, resource management and closing the circulation are missing, etc. The main elements of smart solutions are as follows:

Smart building – Limiting water use besides maintaining appropriate personal and household hygiene, usage of water-saving fixtures and replacement of drinking water quality when not required with rainwater and/or grey water (re-use).

Environmental protection – The transformation of the current rainwater only-drainage system to enable the above domestic and irrigation uses. Increasing wastewater treatment efficiency with special filter systems is a very important task for small cities. The efficient and targeted removal of micropollutants in treated wastewaters with special cyclodextrin-based filter systems. Targeted treatment of hospital and industrial wastewater.

Urban water and energetics - Our goal is to decrease transported water quantities and the system's energy demand, and the utilization of waters and sludge as renewable energy resources and in energy production.

INTELLIGENT URBAN AND RURAL DEVELOPMENT

Our objective is refreshing and 'recycling' knowledge amassed and experienced during centuries and millennia for intelligent – that is, protected, safe, close-to nature, cost effective, therefore sustainable – built urban environment.

The effective tools are the following:

Creating balanced situations, like intensive and harmonic balance between city and nature (green, water); minimizing the effects of weather extremities (puffers in water, energy), and in complementary harmonic balance of buildings and public spaces (sizes and proportions).

Using sustainable construction with seeking and strengthening the regional character of city architecture and architecture matured over the centuries; ensuring natural (comfortable and healthy) living conditions; ensuring sustainable, partially self-sufficient workplaces and buildings with local (obtainable within reasonable distance) and recycled materials.

INTEGRATED INFOCOMMUNICATION (ICT) SYSTEMS

The vision is that all the smart-city areas should be integrated around ICT that allows exchanging all the necessary information between all different areas, all different applications, as well as among all the players of the Smart City. Confidentiality, privacy, security, personality rights and similar aspects are to be strictly obeyed.

Summary

In the significantly differing settings of a small town, these smart solutions are just as required as in a large city. Many settlements are affected in Hungary and the EU. BME EIT is working to become a Center of Excellence of Smart City Solutions, and smart small city integrated developments and business model is one of our topics. As for a large city, individual elements can be selected for the given small city, but these will only become economically sustainable if used integrated with others. And research should take this into account.

Reference

Kovács, K., Bakonyi, P. (2015): Smartpolis project - Establishment of the Smart City Centre of Excellence in the Budapest University of Technology and Economics, Proceedings of the 25th International Conference on Computers and Education, Oct 8-11, 2015, Arad, Romania, pp 177-182. ■

The Identity Theft - A new frontier for hackers and cybercrime [1]

Claudio Cilli

Claudio Cilli is Professor at the Department of Computer Science, University of Rome "La Sapienza".

Current Situation
Disturbing fact: 91% of computers worldwide are infected by Spyware
[ParetoLogic]
Fact: Last Year, nearly 10 million people were victims of identity theft
Fact: On average, identity theft victims spend 175 hours of their personal time and over $800 to clear their names
Fact: The FTC estimates it takes victims 14 to 16 months to clear their names
[Federal Trade Commission, USA]

The Theft of Identity (Internet Identity Theft)

In this article, we will try to illustrate the new and probably most dangerous threat that is incumbent on the citizens – even if they don't use computers and networks to carry out economic commerce or financial operations – when they interact with public and private administrations during their daily life. In truth, this is an old problem: if a person succeeds "to transform completely" into another, even existing, assuming all the characteristics that identify that person in the archives of the various administrations (fiscal registry office, banks, public offices, etc.), s/he can commit criminal action without fear of being discovered. The responsibility will always be attributed to the unaware victim. A famous novel of the Italian writer Luigi Pirandello – "Il fu Mattia Pascal" – shows us the opposite situation, but in some aspect similar: in that novel, the poor victim is given for defunct in the records of the registry office, and she is not able, due to the bureaucracy that does not contemplate such anomalous situation, to demonstrate of being alive and in good health. Therefore, she cannot find a job, open a bank account, etc.

The situation shown by Pirandello was paradoxical at the time in which it was written, but today, when all is done through networked computers, the offices do not exchange printed documents, but only streams of data, and all that we are for the society is constituted by few thousands of bytes, the problem is dramatically real. And we are not speaking of cloned credit cards or swindle via Internet (that however are a consequence), but of something much more serious, as we'll see in the continuation of this article.

Definition

The identity theft can be defined as the use of information about a person obtained, often indebtedness, from Internet, with the purpose to identify himself as that person to make illegal actions. Internet in truth is only the main, but not the only, instrument with which to put into effect the threat, only that its increasing diffusion and the tendency to make use of it to carry out operations that some time ago would have forced us to visit several offices (payment of banking bills, general transactions, signing of contracts) has increased its dangerousness.

Why it happens

The criminals pay always attention to the development of the technologies, much more than the designers do. Before a new instrument is diffused, it's already known how to take profit of its weaknesses for illicit purposes. At the beginning few persons used the ATM, but the tools to make clones of the cards existed; when the data transmission era began and the modems were introduced to allow the computers to communicate, already the hackers had discovered holes in the public telephone network and found the way to make free calls.

The identity theft is only a different means to commit fraud: it is not the objective, but only a means. Progress has supplied the "cyber-criminals" new opportunities to take advantages with devastating consequences. The identity theft can in fact be used to:

- Commit frauds directly. The most innocuous is to use victim's data to obtain access to pornographic or pedophilic sites. The victim will do a poor figure as mini-

1 Part 2 of this article will be published in the Summer Issue.

mum, when penal consequences do not follow. S/he will work hard to demonstrate her/his innocence, and often this will be impossible.

- Be sold to others so they can commit frauds. As it has already happened in the case of the privacy law that has the purpose to protect personal data, thus generating a flourishing market of data banks illicitly created with reserved data about citizens, now placed outside the law. Therefore, we already have proof of data banks, paradoxically sold on Internet, with all the necessary information to impersonate those whose data are within. It's a profitable market that keeps growing.
- Snatch economic information and to spy on bank accounts. It's not a real identity theft, but only use of the snatched information to illicitly inquire in the private sphere of the victim to acquire advantages.
- Open new credit positions. The data of the victim can be used as warranty to obtain lend and advanced financings exceeding personal possibilities or to open checking accounts with several banks "on-line", with greater diffusion each day.
- To generate new forms of illegality.

These are the most diffused illegal consequences of the identity theft, but there is no limit to the criminal fantasy!

How it happens

The identity theft is an extremely sneaky threat that can be put into effect in many ways. Here we bring back only some, but once again, we must reaffirm that there is no limit to the fantasy and to the inventiveness of the criminals.
Here is the list:

- Theft of the pocket/purse that contains documents of identity, credit cards, information, passwords and PINs. These should never be carried together;
- Theft of ordinary correspondence. Also, an error of the mailman who introduces your mail in the wrong mailbox can give the cue to start a crime;
- Interception/reading of e-mail. The protocol used for the e-mail in Internet, SMTP, is intrinsically insecure; it doesn't offer certainty about the authenticity of the sender and it does not prevent that the information in transit might be read by unauthorized users;
- Interception of the data in transit on the computer;
- Penetration in the computer with special programs (spyware) of which we will deal in the continuation of this article;
- Use of personal information supplied to the Internet sites which we register to;
- Obtaining of information from the workplace (theft of financial and personal information) by "hacking" in the files, both recorded in the computer and in paper document or notes, often left unattended;
- Purchase of personal data from illegal data banks. In particular on this point, it must be said that the recent laws on the protection of personal data, in the European Union have generated this new form of illegality, consisting in the creation and sale (or also only consultation by payment) of archives with personal data (e.g.: data regarding the patrimonial state, solvency, consumer profile, etc).

It is not necessary to enter your house to make identity theft

The tiles of the puzzle necessary for the creation of our "social profile" are everywhere:

- Financial information;
- Fiscal data (assurances, taxes, communications with public administration, etc.);
- Personal identifying data and banking information are often stored in the computer, which is a real gold mine for the thief.

How identity thieves use personal information

Here we bring only the main consequences of the identity theft drawn from archives of the investigation agencies and from the denunciations received, but the "applications" of the identity theft are almost infinite:

- Modification of the e-mail address used in the relationships with others;
- Opening of new bank accounts or positions with your identifying data;
- Using the data to obtain approvals or access to pornographic websites that request to demonstrate to be of age by showing a credit card;
- Withdrawal of money from your bank accounts;
- To carry out expenses with your credit cards until the limit of use.

The true damage

It would seem a classic problem of frauds via Internet, but there is more:

- Often the most significant damage suffered by the victims is not of economic type: it is emotional;
- The victims assert that not only they have had to ascertain that their financial privacy has been violated, but that they have had to fight long and hard battles to assert their good faith and to reconstruct the economic and banking position.

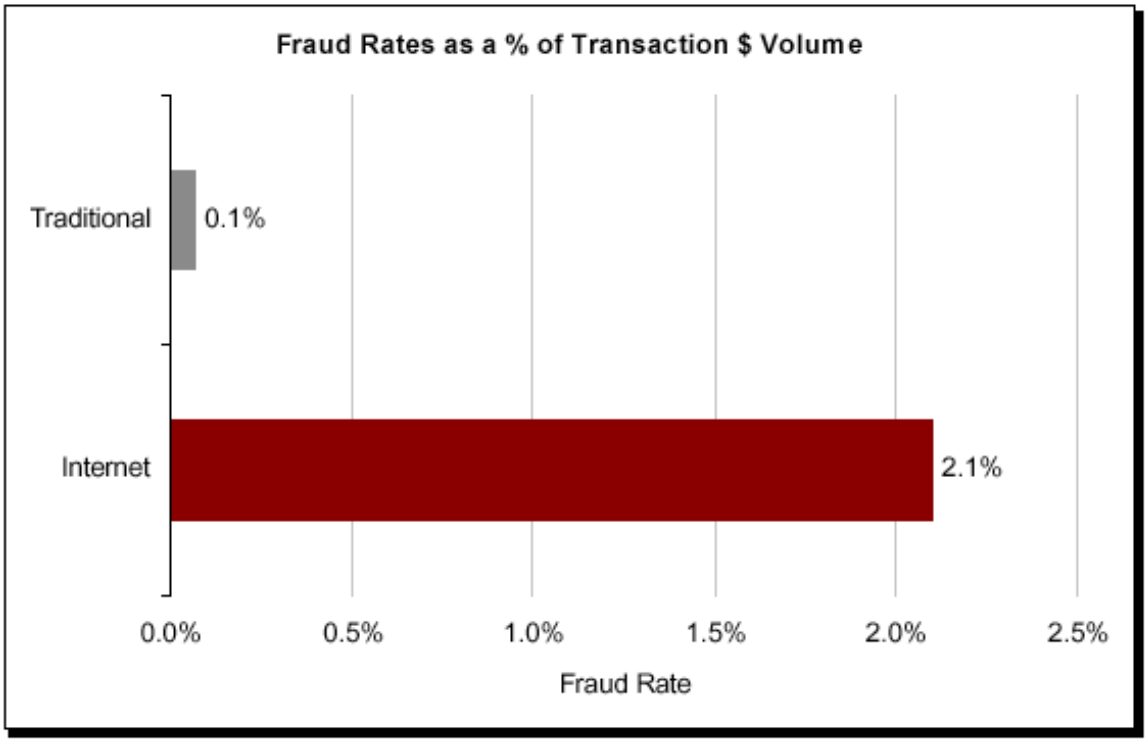
The hacker at work

We continue our treatment with a series of data and some diagrams. The picture that derives represents a disconcert-

ing panorama:

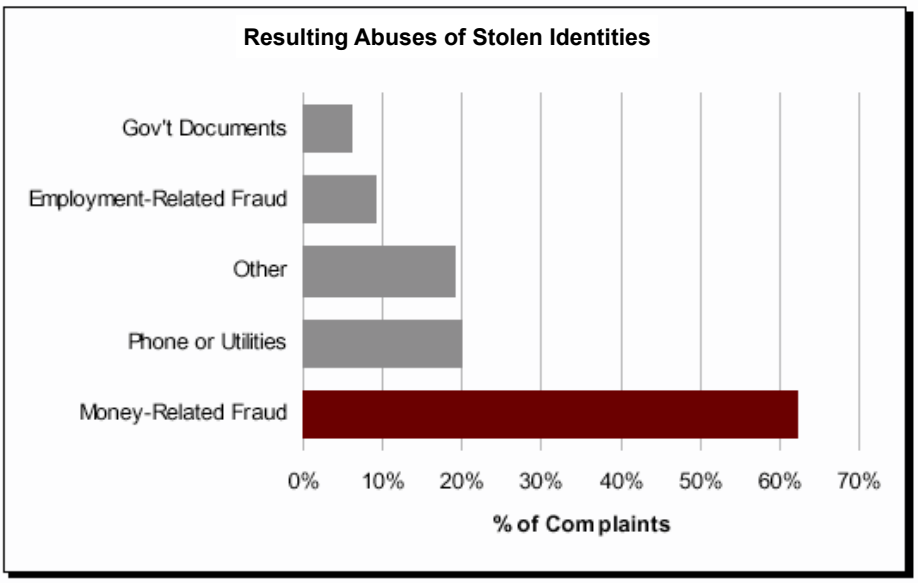
- More than 635.000 denounced cases of attack in 2004,
- 82.094 in 2002, 52,658 in 2001 and 21,756 in 2000 (Source: CERT, 2003),
- About 800% of increase since 2002,
- Symantec has recorded 689 attacks to financial institutions,
- 48% of these were serious (Source: Symantec, 2003),
- Symantec has recorded 616 attacks on e-commerce sites,
- 19% of these with serious consequences (Source: Symantec, 2003),
- 24% of the attacks perpetrated by hackers are intentional,
- 76% are opportunistic (Symantec, 2003).

US Federal Trade Commission's Top Categories in 2004 for Consumer Fraud Complaints	
Identity Theft	**39%**
Internet Auctions	**16%**
Other (miscellaneous)	**12%**
Shop-at-Home/Catalog Sale	**8%**
Internet Services and Computer Complaints	**6%**
Foreign Money Offers	**6%**
Prizes/Sweepstakes and Lotteries	**5%**
Advance-Fee Loans and Credit Protection	**3%**
Business Opportunities and Work-at-Home	**2%**
Telephone Services	**2%**



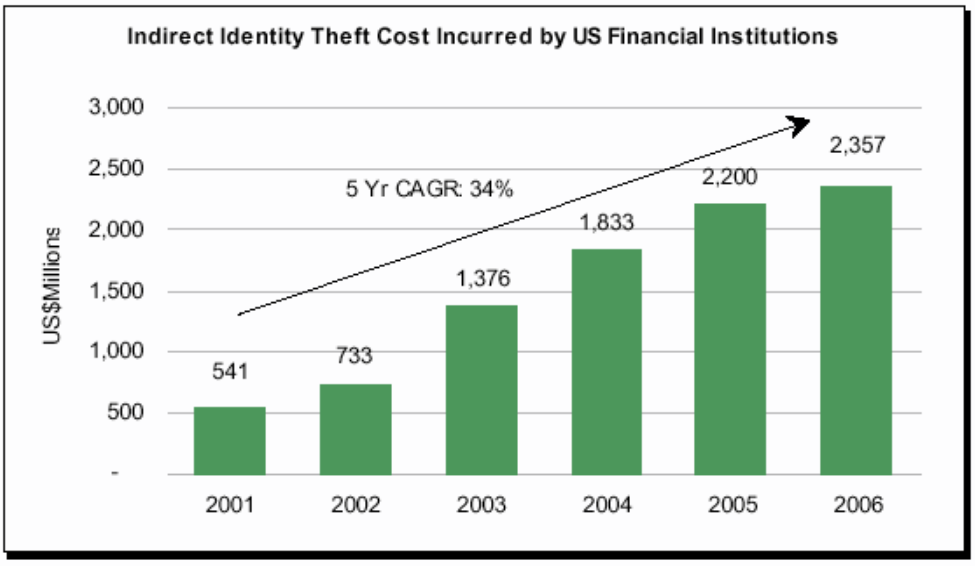
Source: Celent Communications

- More than 200.000 identities are stolen every year,
- The average increase was doubled from 2002 to 2004: from 20,7% to 39% (Source: Federal Trade Commission),
- Internet gave the criminals a new way to snatch personal information, as an example:
  - Criminals created fake eBay site some time ago so that customers entered personal credit card numbers and data (these types of frauds are always more diffused, to the point a name has been given to them: "phishing"),
  - Sites that pretend to offer job opportunities, and ask for a contribution from the customers.



Note: Number of cases: 86,168. Sum of percentages exceeds one because victims can report multiple types of fraud.
Source: Federal Trade Commission

It could be thought that the problem is meaningful only in the United States where the diffusion of the Internet and the computer technologies are very extensive, but this is not exact: in the European Union the identity theft has cost in the last five years more than four billion Euro.
We must, moreover, add a series of negative consequences in terms of image and greater costs, such as the negative impact on the banking system that generates distrust in the customers, the increment of expenses for the computer security and training.



Note: Cost includes dollars spent on technology, legal fees, personnel and training, and consumer education.
Source: Celent Communications

Spam

An analogous problem to the identity theft and serious is Spam. For Spam, we imply a commercial e-mail message with massive sending. Some numerous variants exist: requests for assistance, claims for lottery winnings, worms, etc. In general terms Spam is all that arrives not requested by the addressee, which annoys the recipient. The recipient could reply with a complaint (and thus provide personal data), and therefore declares to exist andplays the game of the sender!

Spam procures an economic damage to the addressee (loss of time to read the message, to delete it, etc.). Spam is the only kind of publicity paid by the addressees even if they do not buy the publicized product. The cost of the shipment is insignificant- it's only to write the message and to send it. The shipment can be automatically done to millions of e-mail addresses, even randomly generated: some might correspond to real persons. In general terms, Spam is "worthwhile" even if only one reader among a million buys the product, and this explains its increasing diffusion.

Various techniques to mitigate the phenomenon have been proposed:

- Making the email sent unattainable,
- Filtering the incoming Spam with proper software. These use two main filtering methods: blacklist (lists of sites from which the Spam messages come and therefore to be automatically deleted in phase of reception, to buy from specialized companies) and "content filtering" (analysis of the content of the messages made by special programs, often based on expert systems, that determine if the message is to be discarded or not). The two methods are not completely secure therefore they are often used in combination.

The possible recourses are based on the application of a provision on the privacy law: it is possible to legally act against the spammer. The Privacy Authority can endorse the spammer. To such purpose the reference norm is the national privacy law.

The general fundamental principles are:

- Prohibition to send without the consent of the interested party,
- Prohibition in any case to send from a not identifiable or not reachable sender,
- Possibility for the Privacy Authority to set up filters,
- It's to be noted that a receiver filtering could be effective also against foreign spammers.

Spyware

Spyware is a technology that helps in obtaining information about one person or an organization without their knowledge. There are more than two hundred and fifty Spyware applications on Internet, that makes it the new, and for this reason the most dangerous, typology of virus.

The prevention is not simple, and it is based nearly exclusively on the knowledge of the problem from the customer's side and on the adoption of adequate policies and procedures aimed to prevent the infections. From a technological point of view, to recognize the presence of a spyware is difficult. The symptoms are not obvious, and often they lack completely. The antivirus programs are not often able to signal their presence, while the anti-spyware programs, like the famous Ad-aware often are not effective, in particular if they are used alone. Removing a spyware is a complex activity that demands great competences. The automatic removal programs are not enough. It is necessary to act manually, on critical system files, like the registry and the configuration.

How to reduce the risk to be victim of an identity theft?

The following checklist with hints and suggestions to limit the risk of an identity theft could be considered

- Limit the information taken with you,
- Do not supply information if you have not requested the service,
- Sign a contract with a identity protection service,
- Know those people to which you are giving personal information on Internet and why,
- Only supply the indispensable information to complete the transaction,
- Make on-line purchases only by known companies,
- Regularly verify the statements of the credit cards accounts,
- Never use a debit card, but only credit cards that allow to contest the expenses,
- Do not supply your company network access password on Internet when it is asked to you to register, but use others. Change them often and do not to use obvious names,
- Regularly update the antivirus software,
- Verify the security patches available for the operating system. Install only those coming from secure and known sources,
- Do not download files from unknown or doubtful sites,
- Use a personal firewall, especially if the Internet access is made by a high speed or DSL line,
- Use a software for the browser that make use of the cryptography for the data sent on Internet,
- Before getting rid of a computer destroy all the personal data it contains,
- Define a policy for the hiring of the staff and consultants,
- Limit the access to company data with a policy based on the "need-to-know" principle,
- Assign every customer an univocal identification code,
- Install and control a network firewall,
- Use the cryptography for all the personal data accessible via Internet,
- Use the cryptography for all the data sent via Internet,
- Do not use the standard security settings supplied by the vendor, but personalize the configuration to your own needs,
- Do not to leave discs, CDs, documents etc. with personal data unattended,
- Destroy in an accurate way data and media no longer necessary,

- Regularly verify the security systems and the procedures,
- Carry out the intrusion tests ("penetration test"),
- Immediately investigate every suspect violation of the privacy or improper use of financial data,
- Only use Internet Service Providers (ISP) that offer assurance of seriousness and security,
- Destroy every document before throwing it,
- Sign the credit cards immediately,
- Destroy the expired credit cards,
- Carry with you only few blank checks,
- Conserve banking, financial documents, taxes receipts, etc. in a secure place, possibly not inside the house,
- Do not to carry with you (if not necessary):
  - Tax identification number,
  - Password and PIN,
  - Passport, birth certificate,
  - Receipts of banking transactions,
  - Personal telephone numbers or of relatives (except those for emergencies).

Conclusion

Spyware is the fastest growing online threat - studies show that 9 out of 10 Internet-connected PCs are infected with spyware. Chances are, your computer is infected, putting your confidential information and your computer's performance at risk. In addition, Spyware and adware programs morph frequently.

The number of identity theft crimes appears to be rapidly growing. Further collection and analysis of complaint data are necessary to better understand the nature of identity theft crimes and to devise effective prevention and enforcement policies. While identity theft has received a great deal of attention in the past few years, we still have much to learn about the crime. Current data sources give some indication of the prevalence of identity theft; however, we need more detailed information about the nature of such theft. Increasing our understanding of identity theft will enable us to determine how successful various prevention and enforcement policies are and allow for development of more effective strategies for combating identity theft.

Considering the above, it appears that the era of Internet is over! Not now, while studies are being conducted aimed to make Internet more secure, there's something we can do now to avoid the consequences of Internet identity theft.

First: follow the rules and suggestions explained in this article, second - although it might sound stupid - when faced with malware on your Pc, the first thing to do is: **Don't panic and don't start deleting files.** Identify the malware and learn as much about it as you can. We have seen people, trying to execute "repairs" without proper information or skills and create more resulting damage than any virus could ever do.

And don't forget the "Golden Rule": Always, always, ALWAYS have a backup!

References

Following is a list of websites where additional useful information can be found:

- American Institute of Certified Public Accountants AICPA overview (http://www.aicpa.org/privacy) and resource centre (http://www.cpa2biz.com/ResourceCenters/Information+Security/Privacy/default.htm)
- Canadian Institute of Chartered Accountants CICA (http://www.cica.ca/privacy)
- International Association of Privacy Professionals (http://www.privacyassociation.org/)
- *WebTrust for Online Privacy* AICPA/CICA (http://www.aicpa.org/trustservices and http://www.cica.ca/webtrust)
- *Article 29 Data Protection Working Party Opinion on More Harmonised Information Provisions* European Union (http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100_en.pdf)
- *Children's Online Privacy Protection Act* (COPPA) United States (http://www.ftc.gov/privacy), *online privacy rule* (http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm), and *consumer guide* (http://www.consumerprivacyguide.org/law)
- *Data Protection Act* United Kingdom (http://www.dataprotection.gov.uk)
- *Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* European Union (http://www.europa.eu.int/comm/internal_market/en/dataprot/law/index.htm)
- *European Union (EU) Directive on Data Protection* (95/46/EC) http://www.dataprivacy.ie/6aii.htm
- *EU Directive on Privacy and Electronic Communications* (2002/58/EC) http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf
- *Freedom of Information Act* (FOIA) United States (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm)
- *Gramm-Leach-Bliley Act* (GLBA) United States (http://www.ftc.gov/privacy)
- *Greece's Data Protection Law (Unofficial English Translation of Law 2472/1997 on the Protection of Individuals With Regard to the Processing of Personal Data)* http://www.dpa.gr/legal_eng.htm
- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Organisation for Economic Co-operation and Development [OECD]) (http://www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.html)
- *Health Insurance Portability and Accountability Act*

(HIPAA) United States (http://aspe.os.dhhs.gov/admnsimp/pl104191.htm), *resource centre* (http://aspe.os.dhhs.gov/admnsimp/) and *consumer guide* (http://www.consumerprivacyguide.org/law)

- *Model Code for the Protection of Personal Information* (Canadian Standards Association, now CSA International, CAN/CSA-Q830-96) (http://www.csa.ca/standards/privacy/default.asp?load=code)
- *Personal Information Protection and Electronic Documents Act* (PIPEDA) Canada (http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html)
- *Privacy Act* United States (http://www.usdoj.gov/foia/privstat.htm) and *consumer guide* (http://www.consumerprivacyguide.org/law)
- Privacy Act Australia (http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108)
- *Privacy Act* New Zealand (http://www.privacy.org.nz/comply/comptop.html)
- *Privacy International and the Electronic Privacy Information Center* Annual review of privacy laws in over 50 countries around the world (http://www.privacyinternational.org/survey)
- *Safe Harbor Privacy Principles* United States (http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm) and *overview* (http://www.export.gov/safeharbor/sh_overview.html)
- *Universal Declaration of Human Rights* United Nations General Assembly (http://www.unhchr.ch/udhr/index.htm)
- Australia Privacy Commissioner (http://www.privacy.gov.au)
- Canada Privacy Commissioner (http://www.privcom.gc.ca)
- European Union National Data Protection Commissioners (http://europa.eu.int/comm/internal_market/en/dataprot/links.htm)
- Federal Trade Commission United States (http://www.ftc.gov/privacy/index.html)
- New Zealand Privacy Commissioner (http://www.privacy.org.nz)
- Ontario Information and Privacy Commissioner (http://www.ipc.on.ca)
- United Kingdom Information Commissioner (http://www.dataprotection.gov.uk)
- Access to justice network (http://www.acjnet.org)
- American Civil Liberties Union (http://www.aclu.org)
- Canadian Marketing Association (http://www.the-cma.org)
- Centre for Democracy & Technology (http://www.cdt.org/privacy)
- Computer Professionals for Social Responsibility (http://www.cpsr.org)
- Consumer Project on Technology (http://www.cptech.org/privacy)
- Consumer Protection Association (http://www.consumerpro.com)
- Consumer.net - Consumer Information Organization (http://www.privacypolicy.com)
- Cookie Central (http://www.cookiecentral.com)
- Cyber-Rights & Cyber-Liberties (http://www.cyber-rights.org)
- Direct Marketing Association (http://www.the-dma.org)
- Electronic Frontier Canada (http://insight.mcmaster.ca/org/efc/efc.html)
- Electronic Frontier Foundation (http://www.eff.org)
- Electronic Privacy Information Center (http://www.epic.org)
- European Union (http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm)
- Health Privacy Project (http://www.healthprivacy.org)
- HIPAA Central Siemens Health Services (http://www.smed.com/hipaa/index.php)
- Identity theft U.S. government central Web site (http://www.consumer.gov/idtheft)
- Industry Canada E-Commerce Task Force (http://e-com.ic.gc.ca/english/privacy/index.html)
- Information Systems Audit and Control Association (http://www.ISACA.org)
- Institute of Internal Auditors (http://www.theiia.org)
- International Association of Privacy Professionals (http://www.privacyassociation.org)
- Internet Law and Policy Forum (http://www.ilpf.org)
- International Security, Trust and Privacy Alliance (http://www.istpa.org)
- Junk Busters (http://www.junkbusters.com)
- Media Awareness Network (http://www.media-awareness.ca)
- National Small Business Poll – Privacy and National Small Business Poll – Advice and Advisors National Federation of Independent Business (NFIB) Research Foundation (http://www.nfib.com)
- Office for Civil Rights (http://www.hhs.gov/ocr/hipaa)
- Online Privacy Alliance (http://www.privacyalliance.org)
- Privacy & American Business (http://www.pandab.org)
- Privacy Exchange (http://www.privacyexchange.org)
- Privacy Forum (http://www.vortex.com/privacy.html)
- Privacy Page (http://www.privacy.org)
- Privacy Rights Clearinghouse (http://www.privacyrights.org)
- Public Interest Advocacy Centre (http://www.piac.ca)

■

MultiCulti

Grado – A place to be

Dorothy Hayden

Biking in the Valle Cavanata Nature Reserve

The Adriatic coast in its northern and eastern part is a region I enjoy a lot, and, in previous NL Issues, I was pleased to take our readers to Venice, Piran and Lovran.

Now, it's a pleasure to guide you to Grado. It takes 90 minutes from Venice to Grado on the E70 Motorway (exit at Palmanova) and just under 30 minutes from Trieste airport. Grado is situated on an island and the approach is spectacular – via a long causeway across the lagoon with some great sights across.

It is a historic settlement in the eastern part of the Marano Lagoon. After the influx of many immigrants from the mainland to the lagoon in the 6th century A.D., it became the seat of the Patriarch responsible for the lagoon islands and Istria. With its 9,000 inhabitants today, it is a functioning fishing port, a spa resort and a major summer holiday destination.

Grado beach (end of May)

Grado is rather full during the active summer season and my personal preference for a visit is May/early June or the second half of September – you can still enjoy the sun, the sandy beaches and shallow sea, and the leisurely feeling, without the crowds.

Just walking with free space around Grado is a feast of the senses. One is overwhelmed by the lightness of feeling in the historic center, with its winding lanes and charming squares, boarded by clustered houses and numerous restaurants with tempting invitations, the picturesque harbor and its fishing boats and hanging nets, the lagoon – dotted with birds and islands, and the far-reaching views of the mountains in Slovenia and Croatia.

Harbor

Grado offers a number of cultural sites to explore, among them the *Duomo* - the *Basilica di Sant'Eufemia*, and the *Basilica di Santa Maria delle Grazie*,… but there's much more to history: if you venture to take a walk along the broad Viale del Sole you will reach the Terme Marine – a thermal wellness center with first-class environment.

Basilica di Sant'Eufemia

10 car-minutes away from Grado is *Aquileia* (on UNESCO's cultural heritage list) – a Roman city, which in ancient times was among the World's largest with a population of over 100,000, but currently has only a few thousand. The main sights there – the Cathedral, built by Patriarch Poppo, and the ancient Roman remains.

Bikers and nature lovers like Grado! There are many places to rent bikes, and the surrounding area offers a variety of routes. I was there last May and chose the one leading to *the Valle Cavanata Nature Reserve*, once a fish-farming area but now a natural reserve and a paradise for birdwatchers. The people at the Visitors Center were great in leading us through the history and the functioning of this reserve. I then biked further on the way to the estuary of the Isonzo, with some excellent places for sea dips and sceneries.

All'Imbarcadero Da Roby in Fossalon di Grado – a first-class restaurant – made the day after some hours of biking. Definitely worth it – one of the best seafood restaurants I have recently visited!

In one of the next Issues I intend to take you to the Kvarner Bay (Croatia), another great place – hang on! ■

Other MultiCulti articles published at http://nl.starbus.org

Verona, Italy (Vol.7, no.1, Spring 2009)

Wachau, Austria (Vol.7, no.2, Summer 2009)

South Tyrol, Italy (Vol. 7, no.3, Autumn 2009)

Rome– San Clemente, Italy (Vol.7, no.4, Winter 2009)

Nesebar, Bulgaria (Vol. 8, no.1, Spring 2010)

Zagreb, Croatia (Vol.8, no.3, Autumn 2010)

Pecs, Hungary (Vol.8, no.4, Winter 2010)

Piran, Slovenia (Vol.9, no.2, Summer 2011)

Lovran, Croatia (Vol.9, no.3, Autumn 2011)

Budapest, Hungary (Vol.9, no.4, Winter 2011)

Riga, Latvia (Vol.10, no.2, Summer 2012)

Salo, Italy (Vol.10, no.3, Autumn 2012)

Baden, Austria (Vol.10, no.4, Winter 2012)

Bari, Italy (Vol.11, no.2, Summer 2013)

Krakaudorf, Austria (Vol.11, no.3, Autumn 2013)

Vienna, Austria (Vol.11, no.4, Winter 2013)

Passau, Germany (Vol.13, no.3, Autumn 2015)

Turin, Italy (Vol.14, no.1, Spring 2016)

Venice, Italy (Vol.14, no.2, Summer 2016)

ICT Development Index

Measuring the Information Society Report, published annually since 2009, features key ICT data and benchmarking tools to measure the information society, including the ICT Development Index (IDI).

IDI 2016 captures the level of ICT developments in 175 economies worldwide and compares progress since 2014. The report assesses IDI findings at the regional level and highlights top performing countries and those that have most dynamically improved their rank in the IDI since 2014. It also uses the findings of the IDI to analyze trends and developments in the digital divide.

The report highlights the role of ICTs in achieving the Sustainable Development Goals (SDGs) and presents the newly agreed SDG indicator framework, including the ICT indicators.

In the IDI 2016 ranking, Korea (Rep.) is first, followed by Iceland, Denmark, Switzerland, UK, Hong Kong (China), Sweden, Netherlands, Norway, and Japan.

IT STAR country ranks are as follows:

- Austria (23)
- Czech Republic (32)
- Slovenia (33)
- Greece (36)
- Italy (37)
- Lithuania (39)
- Croatia (41)
- Slovakia (42)
- Hungary (48)
- Bulgaria (49)
- Poland (50)
- Serbia (51)
- Cyprus (54)
- Romania (60)
- TFYR Macedonia (65)

The full IDI 2016 report is available at http://www.itu.int/net4/ITU-D/idi/2016/ ■

Forthcoming IT STAR Events

IT STAR Business Meeting
May/June 2017
Venue: To be decided

11th IT STAR Workshop
Under consideration - tentative topic: Data Processing
Second half of October 2017, Sofia, Bulgaria

■

IT STAR Partnership Brief

IT STAR is a regional professional ICT related Association in Central, Eastern and Southern Europe, whose 15 members are leading national computer organizations.

Established in 2001, IT STAR has a successfully performing series of *Annual Workshops*, providing a forum to recognized experts from academia, industry, government and professional organizations to debate ICT issues as they relate to education, R&D, innovation and growth, strategies and policymaking. Based on these debates, *Conference Statements and recommendations* are issued and distributed widely within the IT STAR Region and the European Union.

IT STAR supports a *Publications Program* – www.starbus.org/publications including its *Series* with revised and edited proceedings of the IT STAR workshops.

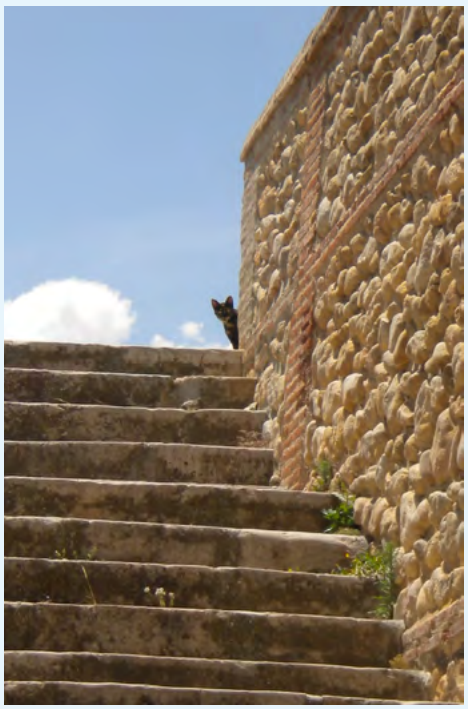
IT STAR's Newsletter (NL) – http://nl.starbus.org is published quarterly and distributed in print form and electronically worldwide – to IT related organizations in business and industry, research and education, government, EU agencies, NGOs and intergovernmental organizations.

Pages 15, and 16 of the NL contain a snapshot of IT STAR and directory of its member societies.

So as to assist the growth of its activities, IT STAR would be interested in considering partnership/sponsorship relations with organizations interested in its portfolio of activities. Areas to consider, include:

- Speakers' slots and visibility within the annual IT STAR events;
- Promotion within the IT STAR publications media – IT STAR's website, newsletter and publications series;
- Joint projects and consultations leading to partnership arrangements with organizations in Central, Eastern and Southern Europe.

For interested organizations –
please contact info@starbus.org. ■



Curious in the IT STAR scene?

This is your place to promote your projects, services and products.

We will help you reach the ICT specialists of Central, Eastern and Southern Europe and beyond.

To advertise in the NL and at www.starbus.org contact info@starbus.org

SNAPSHOT

REGIONAL ICT ASSOCIATION IN CENTRAL, EASTERN & SOUTHERN EUROPE

Type of organization

Regional non-governmental and non-profit professional association in the ICT field.

Date and place of establishment

18 April **2001**, Portoroz, Slovenia

Membership

Countries represented (*see next page for societies*), year of accession, representatives

- Austria (2001) G. Kotsis, E. Mühlvenzl, R. Bieber
- Bulgaria (2003) K. Boyanov, I. Dimov
- Croatia (2002) M. Frkovic
- Cyprus (2009) P. Masouras
- Czech Republic (2001) O. Stepankova, J. Stuller
- Greece (2003) S. Katsikas
- Hungary (2001) B. Domolki
- Italy (2001) G. Occhini
- Lithuania (2003) E. Telesius
- Macedonia (2003) P. Indovski
- Poland (2007) M. Holynski
- Romania (2003) V. Baltac
- Serbia (2003) G. Dukic
- Slovakia (2001) I. Privara
- Slovenia (2001) N. Schlamberger

Mission

"To be the leading regional information and communication technology organization in Central, Eastern and Southern Europe which promotes, assists and increases the activities of its members and encourages and promotes regional and international cooperation for the benefit of its constituency, the region and the international ICT community."

Governance

IT STAR is governed according to the letter of its Charter by the Business Meeting of MS representatives:

2016 Milan, **Italy** (October)
2015 Warsaw, **Poland** (October)
2014 Szeged, **Hungary** (September)
2013 Bari, **Italy** (May)
2012 Bratislava, **Slovakia** (April)
2011 Portoroz, **Slovenia** (April)
2010 Zagreb, **Croatia** (November)
2009 Rome, **Italy** (November)
2008 Godollo, **Hungary** (November)
2007 Genzano di Roma, **Italy** (May)
Timisoara, **Romania** (October)
2006 Ljubljana, **Slovenia** (May)
Bratislava, **Slovakia** (November)
2005 Herceg Novi, **Serbia & Montenegro** (June)
Vienna, **Austria** (November)
2004 Chioggia, **Italy** (May)
Prague, **the Czech Republic** (October)
2003 Opatija, **Croatia** (June)
Budapest, **Hungary** (October)
2002 Portoroz, **Slovenia** (April)
Bratislava, **Slovakia** (November)
2001 Portoroz, **Slovenia** (April)
Como, **Italy** (September)

Coordinators

2015 – Marek Holynski
2010 – 2015 Igor Privara
2006 – 2010 Giulio Occhini
2003 – 2006 Niko Schlamberger
2001 – 2003 Plamen Nedkov (cur. Chief Executive)

Major Activities

- 10th IT STAR WS on IT Security http://www.starbus.org/ws10
- 9th IT STAR WS on ICT Strategies and Applications http://www.starbus.org/ws9
- 8th IT STAR WS on History of Computing http://www.starbus.org/ws8
- 7th IT STAR WS on eBusiness - http://www.starbus.org/ws7
- 6th IT STAR WS on Digital Security - http://www.starbus.org/ws6
- IPTS - IT STAR Conference on R&D in EEMS - http://eems.starbus.org
- 5th IT STAR WS and publication on Electronic Business - http://starbus.org/ws5/ws5.htm
- 4th IT STAR WS and publication on Skills Education and Certification - http://starbus.org/ws4/ws4.htm
- 3rd IT STAR WS and publication on National Information Society Experiences – NISE 08 http://www.starbus.org/ws3/ws3.htm
- 2nd IT STAR WS and publication on Universities and the ICT Industry http://www.starbus.org/ws2/ws2.htm
- 1st IT STAR WS and publication on R&D in ICT http://www.starbus.org/ws1/ws1.htm

Periodicals & Web-site

The IT STAR Newsletter (nl.starbus.org) published quarterly.
www.itstar.eu ■

IT STAR Member Societies

Austrian Computer Society – OCG
Wollzeile 1,
A-1010 VIENNA, Austria
Tel. +43 1 512 0235 Fax +43 1 512 02359
e-mail: ocg@ocg.at
www.ocg.at

Bulgarian Academy of Sciences – BAS
Institute for Information and Communication Technology
Acad.G.Bonchev str.Bl.25A
SOFIA 1113, Bulgaria
Tel +359 2 8708494 Fax +359 2 8707273
e-mail: vomidiv@gmail.com
www.bas.bg

Croatian IT Association– CITA
Ilica 191 E/II,
10000 ZAGREB, Croatia
Tel. +385 1 2222 722 Fax +385 1 2222 723
e-mail: hiz@hiz.hr
www.hiz.hr

The Cyprus Computer Society – CCS
P.O.Box 27038
1641 NICOSIA, Cyprus
Tel. +357 22460680 Fax +357 22767349
e-mail: info@ccs.org.cy
www.ccs.org.cy

Czech Society for Cybernetics and Informatics – CSKI
Pod vodarenskou vezi 2,
CZ-182 07 PRAGUE 8 – Liben
Czech Republic
Tel. +420 266 053 901 Fax +420 286 585 789
e-mail: cski@utia.cas.cz
www.cski.cz

Greek Computer Society – GCS
Thessaloniki & Chandri 1, Moshato
GR-18346 ATHENS, Greece
Tel. +30 210 480 2886 Fax +30 210 480 2889
e-mail: epy@epy.gr
www.epy.gr

John v. Neumann Computer Society – NJSZT
P.O. Box 210,
Bathori u. 16
H-1364 BUDAPEST, Hungary
Tel.+36 1 472 2730 Fax +36 1 472 2739
e-mail: titkarsag@njszt.hu
www.njszt.hu

Associazione Italiana per l' Informatica ed il Calcolo Automatico – AICA
Piazzale R. Morandi, 2
I-20121 MILAN, Italy
Tel. +39 02 760 14082 Fax +39 02 760 15717
e-mail: g.occhini@aicanet.it
www.aicanet.it

Lithuanian Computer Society – LIKS
Geležinio Vilko g. 12-113
LT-01112 VILNIUS, Lithuania
Tel. +370 2 62 05 36
e-mail: liks@liks.lt
www.liks.lt

Macedonian Association for Information Technology – MASIT
Dimitrie Cupovski 13
1000 SKOPJE, Macedonia
e-mail: indovski.p@gord.com.mk
www.masit.org.mk

Polish Information Processing Society
Zarząd Główny
ul. Solec 38 lok. 103
00-394 Warszawa
Tel./Fax +48 22 838 47 05
e-mail: marek.holynski@gmail.com
www.pti.org.pl

Asociatia pentru Tehnologia Informatiei si Comunicatii – ATIC
Calea Floreasca Nr. 167, Sectorul 1
014459 BUCAREST, Romania
Tel +402 1 233 1846 Fax +402 1 233 1877
e-mail: info@atic.org.ro
www.atic.org.ro

JISA Union of ICT Societies
Zmaj Jovina 4
11000 BELGRADE, Serbia
Tel.+ 381 11 2620374, 2632996Fax + 381 11 2626576
e- mail: dukic@jisa.rs
www.jisa.rs

Slovak Society for Computer Science – SSCS
KI FMFI UK, Mlynská dolina
SK-842 48 BRATISLAVA, Slovak Rep.
Tel. +421 2 6542 6635 Fax +421 2 6542 7041
e-mail: SSCS@dcs.fmph.uniba.sk
www.informatika.sk

Slovenian Society INFORMATIKA – SSI
Litostrojska cesta 54
SLO-1000 LJUBLJANA, Slovenia
Tel. +386 123 40836 Fax +386 123 40860
e-mail: info@drustvo-informatika.si
www.drustvo-informatika.si

IT STAR