Italy Country Report

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports, please use the following details: Mr. Jeremy Beale, ENISA Head of Unit - Stakeholder Relations, Jeremy.Beale@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared the **Italy Country Report** on behalf of ENISA: Dan Cimpean, Johan Meire and Marcelo Piccoli.

Legal notice

Table of Contents

Italy

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level*
    - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
        - *National authorities*
        - *CERTs*
        - *Industry organisations*
        - *Academic organisations*
        - *Other organisations active in NIS*
    - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
- *Country specific NIS facts, trends, good practices and inspiring cases.*

For more details on the general country information, we suggest the reader to consult the web site: http://europa.eu/abc/european_countries/index_en.htm

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

E-Government Plan 2012[1]

The President of the Council (Prime Minister) together with the Minister for Public Administration and Innovation unveiled the 'E-Government Plan 2012' in January 2009. The Plan aims at promoting government innovation, spreading online services and reinforcing the accessibility and transparency of the Public Administration, so as to bring it closer to the needs of the citizens and the businesses. The Plan consists of 80 digital innovation projects structured around 4 intervention areas, namely:

- Sectoral, referring to Central Government and Universities;
- Local, covering either the Regions or their capitals;
- Structural, including infrastructure projects, e.g. projects for reducing the digital divide or for improving the accessibility of government services;
- International, to maintain Italy's major involvement in the European-scale networks focused on infrastructures, innovation and best practice dissemination.

The implementation of the Plan is being constantly monitored and its achievements are made public every three months. Citizens can follow the progress status of each planned project via the dedicated website www.e2012.gov.it. Here follows a brief description of the main projects and objectives listed in E-Gov 2012 on NIS:

- Digital interaction between schools and families - simplifying the communication schools/families by putting the main school documents online (e.g.: application for registration; electronic school reports and registers) and making the Internet, email exchange and SMS messages regular communication channels;
- Electronic passport and identity card - the police headquarters and the consulates will deliver the electronic passport with a microprocessor embedded to carry the holder's data and to prevent counterfeiting;
- A certified electronic mailbox for the citizens, the Public Administrations and the businesses with a view to digitise the exchange of documents between citizens/companies and the public authorities.

Strategic Plan for Innovation (Piano Industriale dell'Innovazione)

The Minister for Public Administration and Innovation presented the Strategic Plan for Innovation in October 2008. The Plan aims to promote innovation through:

- Agreements with the central government;
- Agreements with the Regions and the Provinces (local government);
- Infrastructure programmes;
- Special projects,
- Law and standards (amendments to the eGovernment Code on issues such as the medical certificates online, electronic prescriptions, online advertising on institutional sites, the electronic identity card and the National services card, the VoIP -Voice over IP- and the Public Connectivity System -SPC).

[1] *http://www.epractice.eu/en/document/288278*

The regulatory framework

The following Italian national regulations[2] have relevance and applicability in the domain of network and information security:

Decree of 6 May 2009 on the implementation of Law no.2/09

The Decree adopted by the Government (DPCM) on 6 May 2009 with the agreement of the Joint Conference State - Regions (Conferenza unificata Stato Regioni) defines:

- The procedures for delivering the certified electronic mailbox (PEC mailbox) to citizens;
- The procedures for activating the service via a tendering process, paying particular regard to the citizens at risk of exclusion (Article 8 of the eGovernment Code);
- The use of the service and how to withdraw from it.

Law no. 2/09 of 28 January 2009

The law no. 2 on 28 January 2009 converts into law the Decree no.185 of 29 November 2008 which contains measures intended to overcome the economical crisis. The article 16-bis of the Decree states the following:

- Citizens receive a certified electronic mailbox (PEC box) upon request;
- The certified electronic mail is equivalent to a notification by regular mail as mentioned under the article 48 of the eGovernment Code;
- The use of the certified electronic mail is free of charge for citizens;
- Each public administration uses the certified electronic mail for the communications with and the notifications to its employees (of the same public authority or a of a different one);
- The operating rules and the way of delivery of the certified electronic mailbox to the citizens are defined by a decree of the President of the Council of Ministers (DPCM), based on a proposal of the Minister for Public Administration and Innovation.

eGovernment Code

Adopted as a legislative decree on 7 March 2005 and published in the Italian Official Gazette on 16 May 2005, the eGovernment Code ("Codice dell'Amministrazione Digitale") entered into force on 1 January 2006. It aims to provide a clear legal framework for the development of eGovernment and for the emergence of an efficient and user-friendly Public Administration. Laying down a number of rules, obligations, recommendations and targets to promote the use of ICT in the public sector, it is intended to contribute to removing obstacles to further eGovernment development, such as "cultural difficulties" and "obsolete norms".

Among other things, the Code mandates Public Administrations to: share relevant information by electronic means in order to make life easier for citizens and businesses; make a minimum set of contents and services available on their websites, including a comprehensive organisation chart, an email directory, a list of eServices, the possibility to download forms, and details on administrative procedures; communicate by email, namely for the exchange of documents and information; accept online payments from

[2] *Source: http://www.epractice.eu/en/document/288279. The same source was quoted in the case of several Italian laws mentioned in this section.*

citizens and businesses (starting in June 2007); use the electronic ID card and the National Services Card, as standard means of granting access to online services (starting on 1 January 2007).

The Code furthermore grants citizens and businesses with the right to demand and obtain that public administration bodies use electronic means in their day-to-day relations with the users.

In order to facilitate the implementation of the eGovernment Code and accelerate the computerisation of the Italian public offices, the Minister for Reform and Innovation within Public Administration has signed in February 2007 a ministerial order on the interchange of data between Public Administrations and the publication of negotiation activities (the so-called "Innovation Directive").

Data Protection Code [3]

The Data Protection Code was adopted as a legislative decree on 30 June 2003, and it entered into force on 1 January 2004. It replaces the previous Data Protection Law (Law no. 675/1996), as well as a number of other legislative and regulatory provisions.

The Data Protection Code has been meant to update, complete and consolidate Italy's data protection legislation since 1996 by introducing important innovations and conforming national legislation to European regulations, in particular the Data Protection Directive (95/46/EC) and the Directive on privacy and electronic communications (2002/58/EC).

The code aims to strengthen the data protection rights of individuals, allowing them to exercise their rights and instigate proceedings more easily. Individuals do not have to demonstrate that damage or distress has been caused as a result of a data protection breach; they merely have to demonstrate that their privacy has been breached.

The Data Protection Commissioner ("Garante Privacy") is in charge of supervising and enforcing the application of the Data Protection Code. In an effort to simplify the complaints process, the Commissioner has published a complaints form on its website.

Legislative Decree on Electronic Commerce

The Legislative Decree no. 70 of 9 April 2003 came into force on 14 May 2003. It regulates the use of electronic commerce means in Italy as well as the information that eCommerce websites shall compulsorily provide to purchasers.

The Decree transposes the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

Electronic Communications Code

Adopted as a Legislative Decree on 31 July 2003, the Electronic Communications Code entered into force on 16 September 2003. It transposes four of the directives of the EU regulatory framework for electronic communications, the ePrivacy directive being transposed in the Data Protection Code.

---

[3] *Source: http://www.epractice.eu/en/document/288279. The same source was quoted in the case of several Italian laws mentioned in this section.*

Decrees on certified electronic mail [4]

With the Presidential Decree no. 68 of 11 February 2005, emails transmitted through a certified electronic mail (Posta elettronica certificata – PEC) system have acquired legal validity. Another decree, dated 2 November 2005, sets out the technical rules for the formation, the transmission and the validation of certified electronic mail.

Legislative Decree no. 10 on Electronic Signatures

Italy has been among the first EU countries to give full legal value to electronic signatures. The Law no. 59 of 15 March 1997 on the simplification of the Public Administration provided in its article 15 that the use of electronic means would be legally valid for administrative procedures. Rules regarding the use of electronic signatures and documents were further detailed in a series of presidential and government decrees adopted between 1997 and 2001.

The Legislative Decree no. 10 of 23 January 2002 brought the Italian electronic signature regulations into line with the Directive 1999/93/EC on a Community framework for electronic signatures.

Cybercrime legislation

In the early nineties, the Italian Criminal Code was no longer considered sufficient to protect against new forms of crime caused by the increasing use of computer and communications technology. Thus, computer crimes were introduced within the Criminal Code with by Act n°547 of 13 December 1993 concerning modification and integration of the Criminal Code and the Criminal Procedure Code involving cyber crime" (Moficazioni ed Integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica). The legislator did not create a specific section in the Penal Code for new issues, as has happened in some European countries.

Instead they were integrated using the old criteria. Computer system damages were incorporated near common damages, unauthorized access to computer or telecommunication systems near unauthorized access to private property, etcetera. Other criminal provisions related to ICT were introduced by Act. n° 269 of 3 August 1998 regarding Child pornography (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitu), and Act. n° 438 of 15 December 2001 concerning conversion into Law, modifying D.L. n°364 of 18 October 2001, containing urgent provisions to combat international terrorism (Conversione in legge del 18 ottobre 2001, n°374, recante disposizioni urgenti per contrastare il terrorismo internazionale).

Last but not least is Legislative Decree n° 196 of 30 June 2003 that entered into force on January 1 2004, the so called "data protection code", also known as the "Privacy code". It does not specifically concern cyber-crime, but some of its provisions refer to the telecommunications field.

The privacy code is divided into three parts:

- The first part sets out the general data protection principles that apply to all organisations;

[4] *http://www.epractice.eu/en/document/288279*

- Part two of the code provides additional measures that will need to be undertaken by organisations in certain areas, for example, healthcare, telecommunications, banking and finance, or human resources;
- Part three relates to sanctions and remedies. It is expected that the second part of the code will be developed further through the introduction of sectoral codes of practice. Seven codes are planned (including surveillance, with particular regard to video surveillance, human resources, private investigators, and advertising/marketing) which will be developed in consultation with industry groups. The provisions relevant to us are in the second and third part, i.e. articles 167 and 130.

In Italy ICT crime investigations are lead by three main law enforcement bodies: the State Police (Polizia di Stato), the Carabinieri (Arma dei Carabinieri) and the Financial Guard (Guardia di Finanza).

Within the State Police there is a subsection dedicated to postal and communications crime (Polizia Postale e delle Comunicazioni), of which one particular section is devoted entirely to cyber crime investigation.

The Carabinieri have a subsection called the Carabinieri Scientific Investigations Group (Raggruppamento Carabinieri Investigazioni Scientifiche (Ra.C.I.S)), and its Telematics Section (Sezione Telematica) is entrusted with high tech crime investigations. The Financial Guard have the Special Technological Anti-Crime Cell (Nucleo Speciale Anticrimine Tecnologico).

Computer crimes, like any other common crimes, are judged by the Tribunal of First Instance (first court) and the Court of Appeal (appellate court). As a last possibly competent instance there is the Supreme Court (Corte di Cassazione), which rules only on points of law.

Self-regulations

Self-regulatory Code of Conduct for Premium Services and Child Protection[5]

Code of Practice for premium rate numbers in decade 4 – operative guidelines

The Italian mobile telecom operators have adopted a code of conduct that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Italian mobile electronic telecommunications market and complies with applicable European and national legislation.

[5] *Source:* http://www.gsmeurope.org/documents/eu_codes/italy_child_protection.pdf

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	• Ministry of Economic Development — Communications Division • ISCOM • Ministry for Public Administration and Innovation • CNIPA (National Centre for Informatics in the Public Administration) • Italian Personal Data Protection Authority • OCSI • Working Group on Critical Information Infrastructure Protection — Presidency of the Council of Ministers, Department of Innovation and Technology • Postal and Communication Police Service • National Technical Committee on Informatics Security —Presidency of the Council of Ministers, Department of Innovation and Technology • Network Security and Communications Protection Observatory • Department of Emergency Preparedness • Ministry of Interior • Communications Regulatory Authority (Agcom) • National Centre for Cybercrime and Protection of Critical Infrastructure (CNAIPIC) • Committee for the Diffusion of Broadband
CERTs	• CERT-IT • GARR-CERT • CERT-Difesa • CERT ENEL • CERT-RAFVG • GovCERT.IT • S2OC • SICEI-CERT
Industry Organisations	• ICT CE (Associazione Telecomunicazioni, Informatica ed Elettronica di Consumo) • AITech-Assinform • Clusit • Associazione Italiana Professionisti Sicurezza Informatica (AIPSI) - Italian Association of IT Security Professionals
Academic Organisations	• Computer and Network Security Lab (LaSeR)
Others	• Sincert • ISACA Roma • Association of Italian Experts in Critical Infrastructure (AIIC) • EASY • EDEN • ISSA IT • OWASP IT • ISACA IT • Altroconsumo

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who" – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory[6]

[6] *See also the ENISA document:* http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation between national authority bodies

Italy does not have a single institution recognized among NIS stakeholders as the national security agency; there are various organization sharing the responsibilities and competencies concerning the classified information. The Ministry of Economic Development acts as the institution from among all NIS stakeholders in Italy as the one responsible for coordinating the development and implementation of national information security strategy.

Italy is committed to data protection and ensuring compliance in this regard. Italian Personal Data Protection Authority ensures compliance with the Privacy Directive. It is accountable to the Italian Parliament, which has established its powers, defined its statutes and elected its members.

Additionally, Italy has a working group on critical information infrastructure protection, established in 2003 as part of the Prime Minister's Office that composed of representatives from Government departments and agencies, and private sector operators. The country hosts a number of conferences on NIS - events organized prevalently by industry professional and associations.

Other co-operation of NIS stakeholders to combat spam and malware [7]

Cooperation between governmental bodies is in place. In 2003, a permanent observatory group for security and protection of networks and communications was created by the Minister of Communications, the Minister of Justice and the Minister for Internal Affairs. It has generic competences to verify the state of the art regarding network security, including the risks linked to malware and spyware attacks. Up to now the group has performed mainly research activities, as it does not have any real power to enforce legal bans.

The national DPA and the police of communications collaborate on a regular basis to sop and prevent criminal activities involving spam and spyware.

There is also cooperation between government and industry: the working group on privacy, phone interceptions and spam of the national ISPA has the duty to collaborate with the national DPA and to manage the relationships between the two entities.

At international level, the national DPA participates in the CNSA on behalf of Italy.

---

[7] *http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf*

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

In 2003, a permanent observatory group for security and protection of networks and communications was created by the Minister of Communications, the Minister of Justice and the Minister for Internal Affairs. It has generic competences to verify the state of the art regarding network security, including the risks linked to malware and spyware attacks. Up to now the group has performed mainly research activities, as it does not have any real power to enforce legal bans.

The national DPA and the police of communications collaborate on a regular basis to sop and prevent criminal activities involving spam and spyware.

Computer crimes, like any other common crimes, need to be reported to the competent authority before being prosecuted. This competent authority is the Public Prosecutor (Procura della Repubblica). The Public Prosecutor directs investigations and delegates the competent police section to execute the necessary measures.

It is interesting to mention that during the first half of 2009, Italy was mentioned in the global report[8] published by the Anti-Phishing Working Group (APWG)[9] with the following relevant statistics:

- 59 unique phishing attacks reported for this country
- 48 unique domain names used for phishing reported for this country
- A score of 3.9 phish per 10.000 domains registered in this country
- A score of 4.8 attacks per 10.000 domains registered in this country [10]

Emerging NIS risks

The Università degli Studi di Napoli Federico II (Napoli) is an active partner in the FORWARD[11] initiative of the European Commission to promote the collaboration and partnership between academia and industry in their common goal of protecting Information and Communication Technology (ICT) infrastructures.

The FORWARD initiative aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of cyber-threats defenses, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures.

No relevant information was identified on the participation of Bulgarian CERT, ISPs, etc in other European-wide projects aiming at identifying emerging NIS risks, like for example in the Worldwide Observatory of Malicious Behaviours and Attack Threats (WOMBAT)[12].

No other specific input was identified at this stage based on Italian relevant NIS sources.

---

[8] See the report available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf
[9] The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.
[10] See the report available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf
[11] See: http://www.ict-forward.eu/home
[12] See: http://www.wombat-project.eu/

Resilience aspects

A workshop[13] on experimental platforms for Internet resilience, security and stability research was facilitated in 2009 in Italy by the Joint Research Centre[14], on the need to create experimental platforms suitable for conducting empirical security research. Such experimental platforms are expected to enable:

- researchers to use rigorous scientific methods for studying vulnerabilities, threats, systemic faults, potential malicious actions, etc.
- operators and technology providers to try new systems under different security scenarios,
- authorities to better understand the security implications of the Internet infrastructure and the related applications.

No other specific input was identified at this stage on resilience aspects.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive was originally implemented by the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data Act (No. 675 of 31 December 1996) ("Law no. 675/96"). However, Law no. 675/96 has now been replaced by the Consolidation Act regarding the Protection of Personal Data (Data Protection Code - Legislative Decree No. 196 of June 30 2003) (the "DPC").

The competent national regulatory authority on this matter is the Italian Data Protection Authority: the "Garante per la protezione dei dati personali , or the "Garante".

Personal Data and Sensitive Personal Data

The definition of personal data in the DPC is based on the standard definition of personal data and also applies to data relating to legal entities, bodies or associations.

Sensitive data may be processed only with both the data subject's written consent and prior authorisation from the Italian Data Protection Authority (though there are exceptions for religious bodies and trade unions). To this purpose, the Italian Data Protection Authority has issued several general authorisations to the processing of sensitive data.

Information Security aspects in the local implementation of the Data Protection Directive

In addition to compliance with the general data security obligations, the Italian Data Protection Code requires, under criminal sanction, the implementation of specific technical, logical and organisational minimum security measures set forth by a "Disciplinare Tecnico" - "Technical Specifications".

Enforcement and Data protection breaches

The Italian Data Protection Code does not contain any obligation to inform the Italian Data Protection Authority or data subjects of a security breach.

---

[13] *See: http://sta.jrc.it/pdf/scni/ExperimentalPlatforms/ToR_WS_20090619.pdf*
[14] *See the information on the Institute for the Protection and the Security of the Citizen, at: www.jrc.org*

With regard to any breach of the DPC provisions, the data subject may apply either to the Garante or ordinary Court. The Garante may order the stop of the data processing or lay down conditions for the processing. Furthermore, the Garante may impose sanctions or administrative fines. In the event of crimes, the Garante has an obligation to inform the relevant criminal authorities.

Compensation for damages can be requested from the Civil Courts. The Garante has powers of investigation and can also use the Financial Police ("Guardia di Finanza").

NIS awareness at the country level

Italy can be considered as a country where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software.

As an overall assessment, it is possible to say that Italy is in a good position in combating online malpractices. There have been successful prosecutions in spam related cases and the Italian Data Protection Authority recently imposed relatively high fines. Also the DPA cooperates with the police and the national ISPA and participates in the CNSA at international level. Several ISPs offer to their clients spam filters or other security tools. Therefore, a lot of work has been done so far.

However, what seems to be compelling is the rationalisation and simplification of the existing legislative sources (especially in the criminal field: in other words, there are several laws that set criminal sanctions but these rules seem to be often not fully consistent, and therefore there are problems when they have to be applied to real cases) and of the enforcement powers of the relevant authorities. Sometimes, in fact, it is not very clear who is competent for what, and some clarifications by the lawmaker would undoubtedly render the work performed by the Privacy Authority and the Competition Authority more effective. [15]

Awareness actions to combat malware

Administrative decisions – The Italian Data Protection Authority issued an order to clarify the content of legislative provisions in the area of spam. It also issued a number of decisions in the field of spamming, especially in the period 2002-2003, ordering to stop the sending of spam via e-mail/SMS without consent, to stop the use of personal data and/or to provide the claimant with information about the processing of his personal data. In a case where the order was not followed, the DPA denounced the company in question to the competent prosecutor. In 2008, the DPA imposed a fine of 570.000 EUR on an SMS spammer.

Awareness measures – The Police of Communications set up a website where citizens and enterprises can get information about illegal activities that take place on the Internet (including spam, malware and spyware).

Complaint channels – Via the website of the Police of Communications, victims can report cybercrimes. It is not possible to file an online complaint with the national DPA.

---

[15] *Source: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf*

This must be done via regular mail. The completion authority offers a toll free phone number for the reporting of aggressive commercial practices, including spam.

Measures have also been undertaken by the service provider industry: Several ISPs offer to their clients spam filters or other security tools. Telecom Italia, for instance, offers a 'total security' service to its clients against payment of a small fee of around 4 euro/month. This offers extensive protection against spam, viruses, spywares, etc.

Following the traces provided by the ENISA's "Information Package: Raising Awareness in information Security - Insight and Guidance for Member States", the partnership between CNIPA, CASPUR and the "Master in Information Security" is aimed to realize a multimedia project to broadcast guidelines for a conscious and secure utilization of the Internet, as a useful instrument for news, entertainment, communication and other useful and diversified services. Notably, the project is meant to fill the gap between citizens and new technologies, documented in other ongoing projects. [16]

Awareness actions targeting the consumers/citizens

Working within the Safer Internet programme and co-funded by the European Commission, since 2004. Adiconsum and Save the Children have been promoting EASY, a national awareness-raising campaign on safe and responsible internet and mobile phone use among young people. Since the 1st of January 2007, EASY has became the Italian Awareness Centre with the objective:

- To promote safe and responsible use of new media by children and adolescents;
- To promote a culture based on a respect for children using the most diffused technologies, in accordance with the principles sanctioned by the UN Convention on the Rights of the Child.

The centre addresses pre-adolescents, parents and teachers, but its public awareness-raising task is actually much wider in scope, extending also to dealings with institutions, the media and the ICT industry, so that it comprises all the spheres that directly or indirectly impact young people's appropriate use of technological tools, reminding each of them of their specific responsibilities in this area.

A strong network of national stakeholders supports the awareness centre and ensures the dissemination of surveys, educational materials, information and advice.

The Italian Awareness Centre coordinates the Italian celebration of Safer Internet day and cooperates with a large group of stakeholders on a variety of other campaigns.[17]

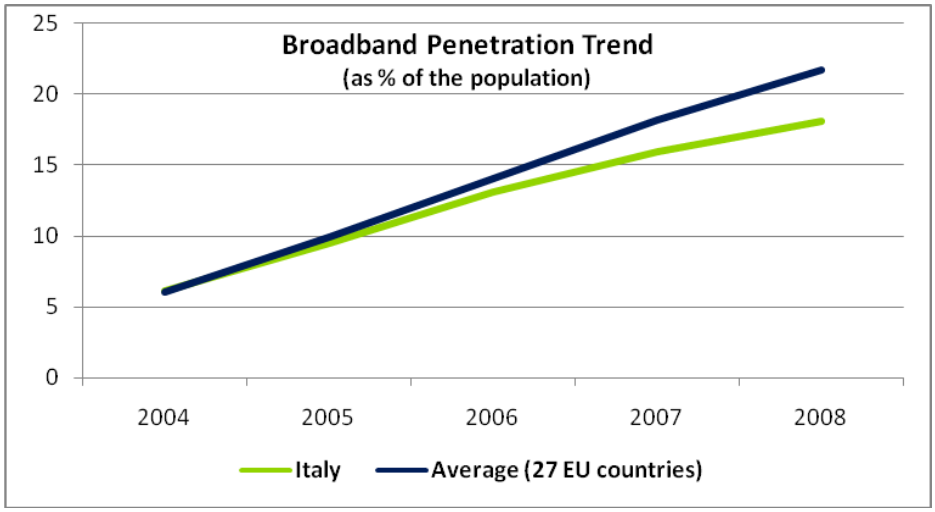
[16] *See the source:* *http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf*

[17] *http://www.saferinternet.org/web/guest/centre/-/centre/italy?p_p_lifecycle=1&p_r_p_1607082367_country=Italy&*

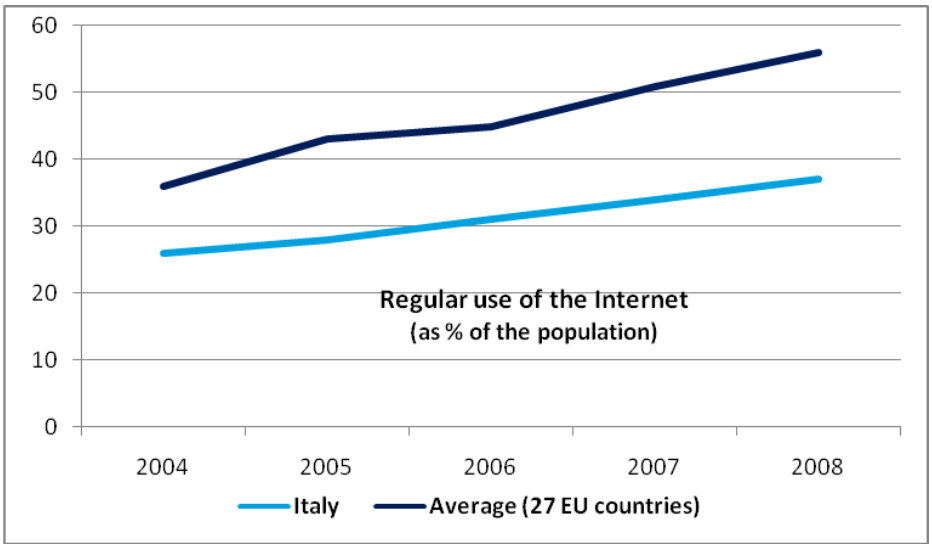
Relevant statistics for the country

The information society in Italy is still at an intermediate stage of development. Although progress has taken place since last year in the areas of broadband and internet usage, there is still significant room for improvement: broadband penetration ranks in line with the EU average, but Internet usage is ranked lower, showing a need of further efforts to narrow the gap with the rest of Europe.

Based on the Eurostat[18] information, it appears that the broadband penetration trend for Italy is currently in line with the EU average:



Based on the same source of information, the regular use of Internet by the population (use as % of the population) is constantly below the EU average but it continues on an increasing path. Rates of internet usage have been gradually improving over the last few years. Nevertheless, take-up of the Internet in Italy is still low and a major segment of the population has never used the Internet. Usage of Internet services is correspondingly low.



[18] *Source: Eurostat*

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry of Economic Development — Communications Division	The functions of the former Ministry of Communications and its inherent financial, material and human resources have recently been transferred to the Ministry of Economic Development. The Ministry of Economic Development: • Supervises postal, financial products and telecommunications services; • Acts as a regulator, coordinator, supervisor and controller; • Represents the government at community and international meetings; • Examines and considers the evolution of opportunities in post and telecommunications, in economic, technical and legal terms at national and international levels; • Takes and publishes technical measures regarding the type of approval and the use of terminal apparatus to be connected, directly or indirectly, to telecommunications networks, granting relevant licences; • Approves telecommunications apparatus; • Grants licences, authorisations and permission, adopting the relevant provisions taking great care of their observance; • Determines technical regulations, considering both users' interests and service quality levels; • Arranges plans for the granting and allocation of radio frequency, granting and allocation, ensuring that these plans are observed.	www.comunicazioni.it www.sviluppoeconomico.gov.it
2. ISCOM	Research activities for and technical body of the Ministry of Economic Development. It acts as notified body under directive 1999/5/EC.	www.isticom.it
3. Ministry for Public Administration and Innovation	The Ministry has been delegated to act on behalf of the Prime Minister in the areas of technological innovation, development of the information society and related innovations for government, citizens and businesses.	www.innovazione.gov.it
4. CNIPA (National Centre for Informatics in the Public Administration)	It provides technical support to the Ministry for Innovation and Technologies. Its main technical areas are: PKI, electronic signatures, ICT awareness, e-government.	www.cnipa.gov.it
5. Italian Personal Data Protection Authority - Il Garante per la Protezione dei Dati Personali	Italian personal data protection authority.	www.garanteprivacy.it
6. OCSI	National security certification and accreditation body. It manages common criteria and ITSEC security certifications	http://www.isticom.it/index.php/qualita-del-servizio/sicurezza-ocsi
7. Working Group on Critical Information Infrastructure Protection — Presidency of the Council of Ministers, Department of Innovation and	Established in 2003 as part of the Prime Minister's Office. The Working Group is composed of representatives from government departments and agencies, as well as private sector operators involved in the management and control of national critical infrastructure.	Not set up.

National authorities	Role and responsibilities	Website
Technology		
8. Postal and Communication Police Service	Established in 1998, the Postal and Communication Police Service has field offices and units operating throughout the Italian territory. Its main activities concern the prevention of and response to computer crime and audiovisual piracy, cop-right protection, protection of postal services. It also acts as a national contact point for transnational emergencies connected with computer crimes in conformity with the specific G8 24/7 network.	http://www.poliziadistato.it/articolo/459-Polizia_postale
9. National Technical Committee on Informatics Security — Presidency of the Council of Ministers, Department of Innovation and Technology	Established in 2002 by the Ministry of Communication and Innovations and Technology Department, the committee is responsible for improving the informatics security of public bodies and for defining their nationwide ICT security plan	Not set up.
10. Network Security and Communications Protection Observatory	Established in 1998, the observatory is made up of members from the Ministry of the Interior, Ministry of Communications and Ministry of Justice. The Internet sub-group deals with investigative and judicial matters relating to the Internet.	Not set up.
11. Department of Emergency Preparedness	The department is responsible for coordinating all initiatives in the event of a crisis.	http://www.protezionecivile.it
12. Ministry of Interior	Oversees aspects as national security, electronic identity (Electronic Passport), and Intelligence and Cybercrime policies.	http://www.interno.it/mininterno/export/sites/default/it/
13. Communications Regulatory Authority (Agcom)	The Communications Regulatory Authority (Agcom) is an independent authority, established in July 1997. Agcom is first and foremost a "guarantor". The two main tasks assigned to it: • To ensure equitable conditions for fair market competition; • To protect fundamental rights of all citizens in Italy.	www.agcom.it
14. National Centre for Cybercrime and Protection of Critical Infrastructure (CNAIPIC)	Unit of the Postal and Communications Police Service specialized against attacks directed towards Critical Infrastructures.	Not set up.
15. Committee for the Diffusion of Broadband	Regional Affairs and Local Autonomies, and Public Administration and Innovation) is to identify the main Public actions needed to promote the diffusion of Broadband services over the Italian territory and to monitor the evolution and availability of those services; to coordinate different projects run out by single Regions; to set guidelines and provide technical recommendations for those projects.	www.comitatobandalarga.it

Computer Emergency Response Teams (CERTs): roles and responsibilities

CERT	FIRST member	TI Listed	Role and responsibilities	Website
16. CERT-IT	No	Yes	CERT-IT is the Italian Computer Emergency Response Team and was founded in February 1994. CERT-IT is a non profit organisation mainly supported by Dipartimento di Informatica e Comunicazione (DICO), Università degli Studi di Milano. CERT-IT became a member of the International Forum of Incident Response and Security Teams (FIRST) in 1995, as the first Italian CERT to be admitted. The main goal of CERT-IT is to contribute to the development of security culture in the computer world, in particular the Italian computer world.	http://security.dsi.unimi.it
17. GARR-CERT	No	Yes	GARR-CERT is the Computer Emergency Response Team for GARR, the Italian Academic and Research Network. It deals with computer and network security incidents.	www.cert.garr.it
18. CERT-Difesa	No	No	The CERT-Difesa mission is to assist the national army in protecting the communication networks and promoting the sharing of information around IT security.	www.cert.difesa.it
19. CERT ENEL	No	No	CERT ENEL is the reference in the Enel group for all problems related to ICT security. Services are provided solely within the company and seek to minimize information risk by ensuring compliance to the legal requirements, corporate standards and international best practices.	www.enel.it/attivita/servizi_diversificati/informatica/cert
20. CERT-RAFVG	No	No	CERT-RAFVG was born in 2005 following the acquisition by the Regione Autonoma Friuli Venezia Giulia, Insiel SpA. CERT-RAFVG acts as a reference point for the activities of cyber security within the region, and as a single contact point of the various components involved in the management of this problem. CERT-RAFVG work in various areas of IT Security to ensure the protection and security of information.	http://cert-rafvg.regione.fvg.it
21. GovCERT.IT	No	No	GovCERT.IT is the public administration computer emergency response team.	www.cert-spc.it
22. S2OC	No	No	CERT established and controlled by Telecom Italia Group.	www.tuconti.telecomitalia.it
23. SICEI-CERT	No	No	Computer Emergency Response Team, responsible for IT security related to Italy's Dioceses.	http://cert.chiesacattolica.it

Industry organisations active in network and information security: role and responsibilities

Industry organisations	Role and responsibilities	Website
24. ICT CE (Associazione Telecomunicazioni, Informatica ed Elettronica di Consumo)	Association bringing together Italian Industry active in telecommunications, informatics and consumer Electronics. Its responsibility is to represent the electronic enterprises that operate in Italy.	http://www.ict-ce.it http://www.anie.it

Industry organisations	Role and responsibilities	Website
25. AITech-Assinform	AITech-Assinform is the Italian association of ICT companies and an affiliate of Confindustria (Confederation of Italian Industry). AITech-Assinform member companies are suppliers of: • Both hardware and software; • Bespoke software development and software customisation services; • Installation and maintenance services; • Technical, application and management support and consultancy services; • Training services; • Outsourcing services; • Network services; • Multimedia content.	www.assinform.it
26. Clusit	Clusit was born based on the experiences of other leading European information security associations such as Clusib (B), Clusif (F), Clusis (CH) and Clussil (L). Clusit aims to: • Raise computer security awareness among companies, public administrations and citizens; • Participate and contribute to the development of laws, practical codes, correct behavior in computer security both at national and international levels; • Contribute to the definition of learning programmes and of certifications for computer security professionals; • Promote the adoption of methodologies and technologies which can contribute to improving information infrastructure security at all levels.	www.clusit.it
27. Associazione Italiana Professionisti Sicurezza Informatica (AIPSI) - Italian Association of IT Security Professionals	AIPSI is a non-profit association founded in 2005 with the scope of representing the community of Italian security professionals. It is the Italian delegate of ISSA (Information Systems Security Association) that counts more than 13.000 associates in 100 organizations around the world. AIPSI activities are: organization of educational forum, documents publication, interactions and links between security experts in order to improve their knowledge, promotion of the correct management of security in public and private organizations.	www.aipsi.org

Academic bodies: roles and responsibilities, tasks

Academic bodies	Role and responsibilities	Website
28. Computer and Network Security Lab (LaSeR)	LaSeR is a research structure of the Dipartimento di Informatica e Comunicazione, at the Università degli Studi di Milano, Italy. The research focus is on applied computer security. In particular, their interests range from vulnerability analysis (both in web applications and executable code) to malware analysis and intrusion detection.	http://security.dsi.unimi.it
29. Università degli Studi di Napoli Federico II		www.international.unina.it
30. Istituto Italiano per la Privacy (IIP)	The Istituto Italiano per la Privacy (IIP), or Italian Institute for Privacy, is a research center dedicated to	

Academic bodies	Role and responsibilities	Website
	the thematics of cybersecurity and protection of personal data in global ICT society. IIP is founding partner of the European Privacy Association.	
31. Institute for the Protection and the Security of the Citizen	Joint Research Centre	www.jrc.org

Other bodies and organisations active in network and information security: role and responsibilities

Others	Role and responsibilities	Website
32. Sincert	National system for the accreditation of certification and inspection bodies.	www.sincert.it
33. ISACA Roma	No-profit association for security experts, mainly interested to Educational activities.	www.isacaroma.it
34. Association of Italian Experts in Critical Infrastructure (AIIC)	No-profit organization with the intent of promoting in Italy many activities in the field of Critical Infrastructures, their security and interdependencies: • Research; • Education; • Analysis of risks; • Awareness; • Consulting services.	www.infrastrutturecritiche.it/aiic
35. EASY	Part of the European 'Insafe' Internet safety network under the 'Safer Internet' programme which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user, as part of a coherent approach by the European Union.	http://www.easy4.it/component/option,com_contact/task,view/contact_id,2/Itemid,86/ www.easy4.it
36. EDEN	Part of the European 'Insafe' Internet safety network under the 'Safer Internet' programme which aims to promote safer use of the Internet and new online technologies, particularly for children. Its goal is also to fight against illegal content and content unwanted by the end-user. The initiative is part of the EU's coherent approach.	http://eden.saferInternet.it
37. ISSA IT	The Information Systems Security Association (ISSA) is a not-for-profit, international organization of information security professionals and practitioners. The mission of the ISSA is to enhance the knowledge and skills of its, encourage exchange of information security techniques, approaches, and problem solving, be the global voice of the information security professional, and promote best practices in information security. Italy ISSA Chapter (ISSA IT) is an independent chapter of the Information Systems Security Association (ISSA). It facilitates, among other things, knowledge sharing events on various information security topics throughout the year in Italy.	www.aipsi.org

Others	Role and responsibilities	Website
38. OWASP IT	The Open Web Application Security Project (OWASP) is an open-source application security project with local chapters. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. OWASP advocates approaching application security by considering the people, process, and technology dimensions. The chapter in Italy organizes local events such as the Mini-meetings, chapter meetings and specific events.	www.owasp.org/index.php/Italy
39. ISACA IT	ISACA is a Worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems. The chapter in Italy organizes local events such as education and training, workshops, roundtables and other specific events.	www.aiea.it
40. Altroconsumo	A consumer organisation, its aim is to protect and educate consumers.	www.altroconsumo.it

Country specific NIS glossary

AIPSI	Associazione Italiana Professionisti Sicurezza Informatica is the Italian Association of IT Security Professionals
CNIPA	National Center for the Information of the Public Administrations -Centro Nazionale per Informatica nella Pubblica Amministrazione
DPCM	Decree adopted by the Government
DPA	Data Protection Act
EHR	Electronic Health Record
ICT CE	Associazione Telecomunicazioni, Informatica ed Elettronica di Consumo is the association that represents the electronic enterprises that operate in Italy.
LaSeR	LaSeR is a research structure of the Dipartimento di Informatica e Comunicazione, at the Università degli Studi di Milano, Italy.
MePA	Centralised eMarketplace accessible to all Italian Public Administrations - Mercato Elettronico della Pubblica Amministrazione
Personal Data	The definition of personal data in the DPA is similar to the standard definition of personal data. In particular, it should be noted that the DPA only applies to individuals as opposed to legal entities.
SPC	Public Connectivity and Cooperation System

References

- An overview of the eGovernment and eInclusion situation in Europe, available at http://www.epractice.eu/en/factsheets
- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Italy - ENISA CERT Directory: http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/italy
- The "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator" published by the Italian Personal Data Protection Authority, available at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1628774

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu