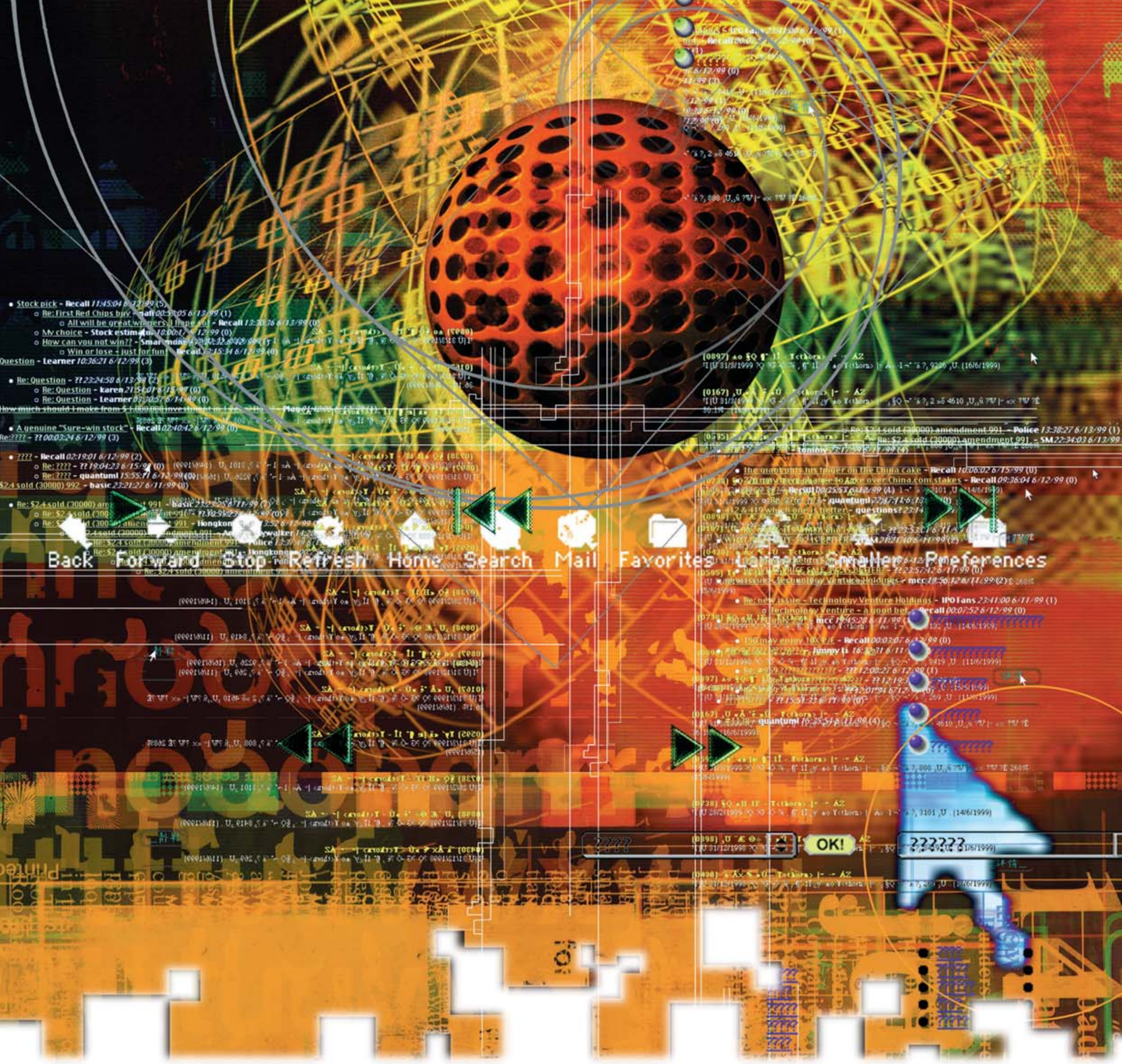


Provider Security Measures Part 2

Security and Anti-Spam Measures of Electronic Communication Service Providers - Status and Outlook

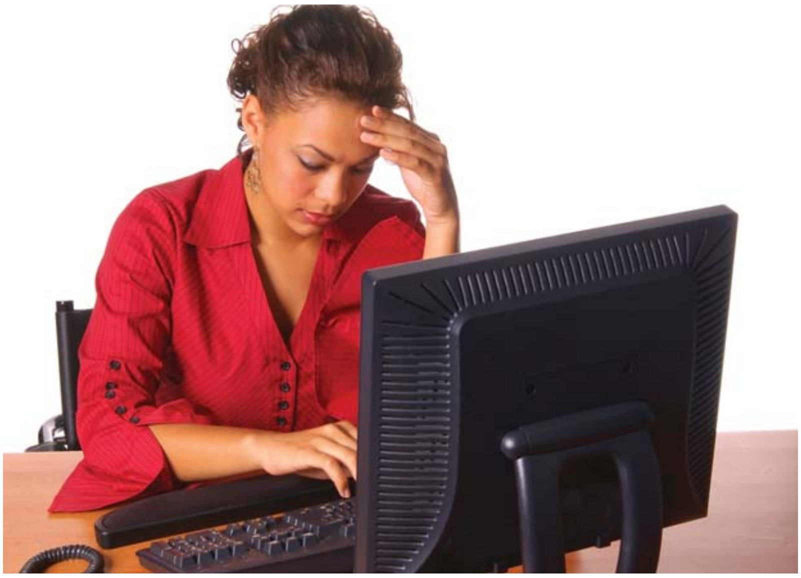
Deliverable 4.2.b of ENISA's Work Program 2006
ENISA/TD/SP/06/118

Carsten Casper & Pascal Manzano

European Network and Information Security Agency
Technical Department – Section Security Policies

June 2006

enisa
European Network and Information Security Agency



Index

1 Executive Summary

Providers of electronic communication services are in the spotlight when it comes to Internet security. European citizens and enterprises have to trust them before they engage in commercial or social transactions online. However, spam and security incidents continue to hinder communications. Indeed, a lack of trust is having a severe impact on the information society in Europe. To improve this situation, the EU has provided a legal framework for electronic communication services and how to secure them.

This report describes how providers have taken into account these legal requirements and what can be done to further secure European networks and services. It is based on surveys that ENISA conducted among providers as well as information gained from conferences and workshops. It focuses on recent developments and trends rather than on detailed statistical data. The facts, conclusions and proposals in this report are grouped under three main themes:

Study - Overview

Increasing transparency	Defining appropriate security	Setting standards
• Reporting of security breaches • Becoming aware of a security or spam problem	• State of the art and cost of implementation • Email security versus privacy	• Technical and organisational security measures • Measures to fight spam

Increasing transparency

Reporting of security breaches – While reporting is to some extent mandatory in the US, reporting in the EU is mostly on a voluntary basis. Meaningful metrics and shared data on security incidents are necessary to increase the transparency of information security and to plan for appropriate and efficient countermeasures.

Becoming aware of a security or spam problem – Many security problems go unnoticed. While the visible level of spam continues to be very high, the nature of the threat changes. More and more spam is unknowingly sent from citizens' computers acting as so-called 'zombies'. Brand names are hijacked and dubious registrars fool domain holders. Some providers see data on threats as proprietary information that gives them a competitive advantage. Furthermore, many still rely solely on complaints from customers rather than proactive network monitoring. They also fail to inform customers about the cost of countermeasures. Providers have to deepen their analysis of incidents, while Europe in general needs a warning mechanism to identify and address upcoming threats.

Defining appropriate security

State of the art and cost of implementation – Most providers follow so-called industry best practice. Many offer free spam filtering or hotlines, even at great cost to themselves. Reported data on damages from security incidents are rare, making a cost-benefit analysis difficult. Providers also have to improve customer confidence, for instance by showing compliance with security certificates. Further EU research is necessary.

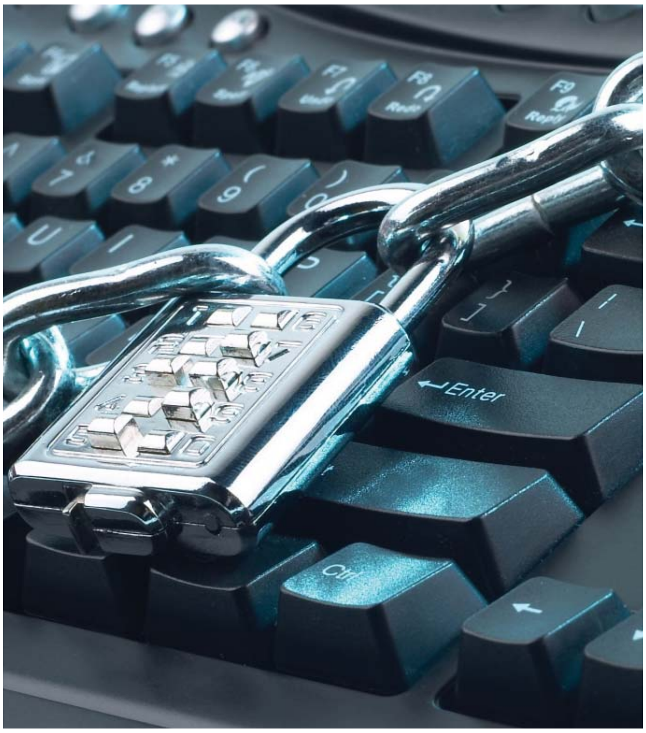
Email security versus privacy – Providers see a conflict between delivering secured services and protecting privacy. Opinion 118 of the Article 29 Working Party on privacy helps find the right balance between these conflicting goals. Still, the cost of widespread customised filtering is prohibitive and a further dialogue is necessary between privacy and security proponents.

Setting standards

Technical and Organisational Security Measures – The goal is not to find, but rather to refine security measures. Quarantining infected computers, securing the Domain Name Service and protecting neighbouring networks should be on the technical agenda. Providing clear contact details, offering detailed guidance to subscribers and raising awareness about identity theft helps secure communications from an organisational perspective. Consumer training could be provided in public-private partnerships. Measures depend on the type of business, the size and the maturity of the provider.

Measures to fight spam – In the EU, various anti-spam laws are in place. The challenge is to enforce them, in Europe and beyond. The OECD Anti-Spam Toolkit, codes of conduct for providers, sender authentication techniques, fines for spammers and initiatives on collecting data on spam all play a role. Fear of counter-lawsuits from spammers, the prospect of additional income from dubious email marketing services and the burdensome reporting of spam cases continue to challenge some providers. Awareness about spam and related security threats must remain high.

The following report is a deliverable of ENISA's Work Program 2006. This research will be continued in 2007.



2 Introduction

2.1 Motivation

The European citizen does not yet feel secure when using the Internet, although much has already been done to make the Internet a safer place to communicate, to interact with governments and to do business. It is necessary to document security measures taken and communicate the results of these improvements to the European audience.

In particular, Internet Service Providers (ISPs), telecommunication companies and other content and service providers play a major role in securing the Internet. They have implemented a wide range of security and anti-spam measures, not only following their own risk assessment and cost/benefits analysis, but also in response to national legislation and written guidance on information security. Many of these have been put in place following European Directives, in particular the European Directive 2002/58/EC ("Directive on privacy and electronic communications") and the regulatory framework Directives for electronic communications (2002/19-22/EC).

This deliverable from ENISA reports on the current status in Europe and provides an outlook on the future. It aims at increasing trust in electronic communications among businesses, governments and citizens of Europe, leading to a higher acceptance of eGovernment and eCommerce services. This is necessary to achieve the goals of the i2010 initiative, creating an open and competitive single market for information society and media services within the European Union.

2.2 Methodology

This paper is the second part of deliverable 4.2.b of ENISA's Work Program 2006, referred to as a *"Study listing measures adopted and made available by providers of electronic communication services to comply with legal requirements regarding technical and organisational measures to safeguard the security of their services"*, envisaged for the second quarter of 2006. The first part was delivered in February 2006, following a request from the European Commission (20051103_COM) to start working on this issue as early as possible and to deliver results before the deadline that was originally planned (2Q2006). This first study, conducted at the end of 2005/beginning of 2006, is subsequently referred to as the "ENISA Survey". It has the reference number ENISA/TD/SP/06/0055.

Consequently, ENISA adjusted the focus for this report. Complementing the first study with more data points and slightly adjusted questions, this report is based on data from the first study, from a number of workshops and conferences that ENISA has attended since its inception and on extensive Internet research.

The report is organised around six major themes – topics that are most relevant, most neglected or most controversial. For each of the themes, it provides facts and observations, evaluations and conclusions, and advice and proposals.

The facts and observations section is a summary of ENISA's own studies and other data sources. Rather than listing all available data, this section focuses on recent trends and interesting data points. The information is given as-is, with short reference to the source. A detailed list of references, including web links, is included in the appendix.

The evaluations and conclusions section describes the opinion of ENISA. Beyond the facts, they explain the reasoning behind why ENISA chose to list the data points above, and they prepare the basis for the third section. There is not always a direct link between the statements of the three sections; several statements have to be seen together.

The advice and proposals section provides a draft for solutions. This can range from an early idea that needs further discussion with stakeholders and partners of ENISA to a strong proposal whose implementation ENISA will support with its weight in the European security community. This can pave the way to refined legislation, or at a minimum it will bring additional projects, workshops and deliverables from ENISA itself.

Note that the recommendations in this report do not replace the recommendations in the February 2006 report.

The report has been designed to bring concise and hopefully new information to the educated information security community. It is neither the definitive best practice guide on spam fighting, nor a general blueprint for future security legislation. It is merely a contribution to understanding the challenges that providers face, an outline of solutions that leading providers take – and that others may want to adopt – and an attempt to make the reader (re-)gain trust in electronic communications in Europe.

2.3 Overview

The security of electronic communications services is a complex topic. There are technical, legal, organisational, political and business aspects. The issue of tackling spam is equally complex, but even more dynamic as threats and countermeasures evolve quickly. There is no one solution. Any paper on these topics has to address a variety of perspectives and opinions.

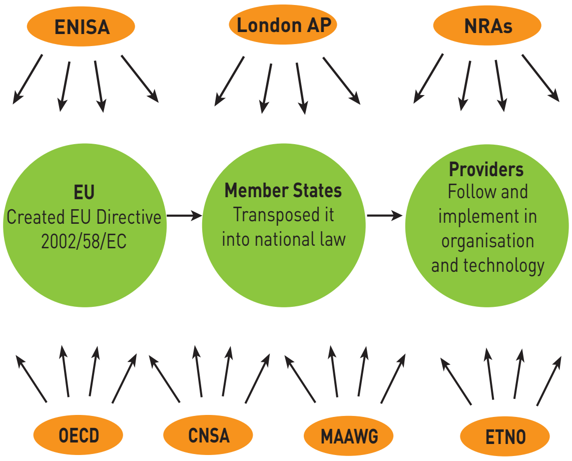
This document describes the current status of security and spam in electronic communications services and predicts their potential development in the next two years. It does so by grouping dozens of data points, observations and proposals under three main themes.

"Increasing transparency" has been identified by ENISA as the most crucial aspect. The information security community still needs to learn more about the current situation in European networks and the motivation of all players. It is especially relevant, because a number of projects are underway that could help increase transparency. Actual achievements are within reach.

"Defining appropriate security" has been a goal at least since Directive 2002/58/EC came into existence. However, owing to cost and state of the art, it is often paid only lip service and, even when processes for defining security are drafted, they are rarely executed. It is difficult to see how major advances can be made in the short term, although some progress with regard to privacy vs. security is visible.

"Setting standards" is a topic of ongoing discussion. Here the challenge is to stay informed about recent initiatives and developments both in the technical and political arena. Significant progress has been made in the past three years, but it is not yet time to shift the focus. Security measures and anti-spam measures require continuous attention.

Shaping information security and anti-spam measures in Europe


ENISA
London AP
NRAs
EU
Created EU Directive 2002/58/EC
Member States
Transposed it into national law
Providers
Follow and implement in organisation and technology
OECD
CNSA
MAAWG
ETNO

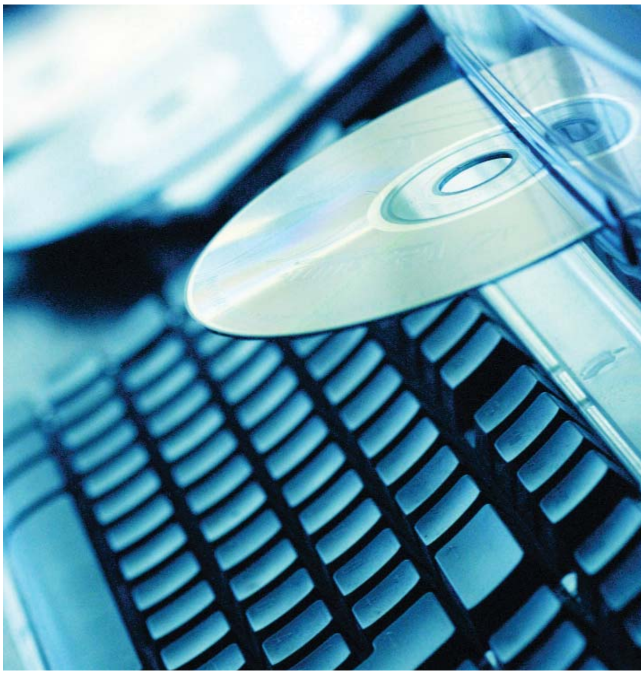
The general guideline for this report is European Directive 2002/58/EC. It was used to structure the questionnaire which was the basis of the first survey. Moreover, some of the themes of this report link directly to the Directive, especially Article 4 and Article 13. However, the Directive is not directly applicable to providers of electronic communication services, who are the main group under discussion in this paper. The 25 Member States of the European Union transpose a Directive into national laws, and only these laws are binding for providers in the EU. In addition, there are a number of groups and initiatives in the information security community which provide additional guidance with regard to the Directive, the laws and their implementations by providers.

3 Increasing transparency

"If you cannot measure it, then you cannot manage it", is common wisdom in corporate management. How can we manage information security if we still have so few data points and – more importantly – if these are not comparable? How can we decide on countermeasures if we do not have a clear – and timely – picture of what the problems are? Becoming aware of security risks is a necessary starting point; sharing this information with peers or reporting it officially is the complementary step.

3.1 Reporting of security breaches

Reporting of security breaches is a sensitive and heavily discussed topic. Not only is there disagreement as to whether and how reporting should take place, there is also no widely accepted definition of what a security breach is. A targeted port scan, a sniffed password, a web site defacement and a large-scale credit card fraud can all be considered breaches. It should also be noted that there is a difference between 'a breach' (a successful attack) and 'a risk of a breach' (a vulnerability) as mentioned by EU Directive 2002/58/EC.



Reporting of security breaches

- Make reporting of breaches prevalent and data comparable
- Keep vulnerability research motivated
- Promote metrics
- Provide information to customers
- Incoming spam vs. outgoing spam
- Promote information sharing

Facts and Observations

- Most providers decide by themselves if and how subscribers and others should be informed. Around half of providers **inform customers** about the risk of a breach via private channels (i.e. private web site, email or mail). Very few report to the public (e.g. by publishing on the web site or in a press release). Only in Finland are providers requested to report to the Finnish National Regulatory Authority (NRA). (ENISA Survey 2006)
- California's State Bill 1386, which made **reporting of security breaches** that involve Californian citizens **mandatory**, went into effect on 1st July 2003. Following this example, 30 other US states passed a similar law. 20 of them come into force between 1st January 2006 and 1st January 2007. As a result, a number of high-profile breaches became public and raised awareness of identity theft in the US.
- **Vulnerability research** becomes more and more **commercialised**. A market develops, where security researchers do not inform the public, but rather give the information only to security companies which pay them. (Symantec's Internet Threat Report 3Q2006)
- The '**Time to Compromise**' describes how long a computer system without protection can be connected to the Internet before it gets compromised. This is a metric that illustrates the need for patches. The Time to Compromise for a system varies, depending on the ISP's policy and the filtering rules of neighbouring systems. (Symantec's Internet Threat Report 3Q2006)
- Although most UK businesses have procedures in place to log and respond to security incidents (83%), only a small number maintain evidence to legal standards (21%) or can deal with claims that an outsider has taken control of the network (22%). (DTI Report 2006)
- To promote the disclosure and sharing of cyber-security information amongst firms, the US federal government has encouraged the establishment of many industry-based **Information Sharing & Analysis** Centers (ISACs) under Presidential Decision Directive 63. (From "The Economic Consequences of Sharing Security Information", 2005)

Evaluations and Conclusions

- It seems that the reporting of breaches increases transparency, encourages countermeasures and helps decrease the overall number of breaches. However, comparable quantitative data that would underpin this assumption are missing.
- In most of Europe, reporting of breaches is not seen as mandatory and is not formalised. If there is no common approach for measuring and reporting, data cannot be shared.
- Commercialised vulnerability research has two effects. On the one hand it is an incentive to spend time and other resources on research, thus helping the community to identify security problems. On the other hand, vulnerability information is no longer shared freely between researchers, so the risk posture will become more difficult to judge. It is important to have a co-ordinated vulnerability publication process so that vendors have sufficient time to provide patches.
- There are a number of measures that providers could take to help identify and communicate security breaches, for example they could install honey-pots and honey-nets to trace hackers' activities or monitor unused IP address space. ISPs could also measure the Time to Compromise for selected vulnerabilities on a regular basis and share or report this information. This would allow providers to co-ordinate their policies, rewarding those providers who help increase the Time to Compromise and shun those who do not. It would also allow countries to some extent to describe their security posture, assuming that providers take their measurements within geographic borders.

Advice and Proposals

- **Providers** should start reporting to NRAs or to a trusted third party on a voluntary basis, using a set of agreed metrics.
- **Member States** should encourage or require the reporting of security breaches.
- **The EU** should introduce a range of guidance and/or legislation that provides incentives for the reporting of security breaches or even makes it mandatory.
- **ENISA** should initiate a partnership for collecting information about trends and the volume of security breaches, including possibly ENISA itself acting as an Information Sharing and Analysis Centre.
- A regulated market of vulnerability research is currently not an option. However, the EU must keep an eye on the development of commercialisation. A co-ordinated vulnerability publication process is important, balancing full disclosure (which puts pressure on vendors to issue patches) and controlled disclosure (which particularly allows critical infrastructure implementations to be secured before the vulnerability is made public).

3.2 Becoming aware of a security or spam problem

Before a provider can report on security breaches or massive spam problems, it has to become aware of them. Ideally, the provider would investigate the origin of the problem, the cause and the impact to its own infrastructure. The provider can monitor the network proactively or wait until someone reports the problem.

Becoming aware of a security or spam problem

- 80% of all emails are spam
- Most of today's spam is sent via zombies
- EU countries receive more spam than they send
- Zombie networks are getting smaller
- Providers still rely too much on complaints

Facts and Observations

- Almost two thirds of all emails that European providers **receive** are spam, while **outgoing spam** accounts for only about 5% of all emails (ENISA Survey 2006). However, some reports also indicate that more than 20% of all spam worldwide originates from Europe (see section "Measures to fight spam").
- **80% of all email is spam**, based on an evaluation of approx. 390 million mailboxes worldwide. (MAAWG Email Metrics Program 1Q2006)
- 80% of spam is **sent via zombies**, according to a vendor report from 2004 (Sandvine). This figure is still widely accepted. (MAAWG Conference)
- To a large extent, **providers rely on complaints** from subscribers to become aware of spam or security problems. In addition, providers cite complaints from other ISPs as a source of information. (ENISA Survey 2006)
- More than half of providers inform customers of remedies that they can take, but very **few providers inform** them about the associated **costs**. (ENISA Survey 2006)
- Providers observe more targeted malware. Hackers plan that such malware has only a short lifespan and they use only a few hundred zombies to **stay under the radar** of network monitoring. (MAAWG conference)
- Some providers see information about fraudsters etc. as **proprietary and competitive information** and do not want to share it.
- There are more than one hundred **hijacked brands**, several hundred unique password stealing malicious code applications, more than one thousand password stealing malicious code URLs and up to ten thousand new phishing sites every month. (APWG Phishing Activity Trends Report, February 2006)
- Some **dubious registrars** also try to trick domain holders into changing their registrar and registering with them. This scheme is hardly any different from phishing.
- There are ongoing discussions at ICANN to **close public access to the WhoIs database** in order to protect the privacy of domain owners. WhoIs databases are an important first step in identifying spammers. According to Spamhaus, even bogus entries in the WhoIs database help identify spammers. (MAAWG Conference)

Evaluations and Conclusions

- According to ENISA's observations, the spam/email ratio in Europe is only slightly better than the measurement of the (US-dominated) Message Anti-Abuse Working Group (MAAWG). Figures have reached a high level and a mailbox without any spam-protection is practically useless.
- While some reports indicate that spam coming from Europe has decreased, others show that it is on the rise. Both may be true. The legal situation makes it difficult for spammers to hide in the EU. However, technically their emails might still come from Europe – and increasingly they do. This must be attributed to an increased rate of bot-net infections, facilitated by an ever larger number of flat-rate always-on broadband connections in Europe. That is, while most spammers are located outside the EU, the infrastructure that they use – bot-nets of hijacked consumer PCs – is located in countries like France, Spain and Poland.
- The spam problem is multi-dimensional. Dealing with spam requires a technical approach both on the sending side (i.e. with regard to bot-nets) as well as on the receiving side. Dealing with spammers requires an enforced legal framework that allows for legitimate direct marketing and removes incentives for spammers, i.e. sets fines that are a real counterbalance to the income from spam.
- Increasingly security breaches and spam are not separate topics. A breach happens when an infected email attachment installs a Trojan on a computer, and spam is often sent from a bot-net which is the result of a number of security breaches.
- Current and emerging risks such as domain kiting or domain registration scams evolve quickly (see section "State of the art and cost of implementation"). In order to find the appropriate political, regulatory or technical response, Europe needs fast and co-ordinated warning and information mechanisms.
- Some providers rely only on complaints from subscribers. For a timely response, a more proactive approach is necessary, taking into account complaints from subscribers as well as continuously monitoring traffic. Indeed, most providers pursue such a combined approach. It is encouraging that providers also react to complaints from other providers. However, the ratio between partner complaints, subscriber complaints and problems identified by monitoring is not yet clear and requires further analysis.

Advice and Proposals

- With regard to problem identification, **providers** should rely first on their own monitoring capabilities, second on complaints from other providers and only then on complaints from subscribers.
- **The EU** should support the positive identification of email senders (e.g. SIDF, DKIM). Providers should implement it as soon as possible and in a cost-efficient manner.
- **Providers** should be encouraged (if not requested) to monitor their networks proactively rather then reacting only to complaints from customers.
- **ENISA** should deepen the analysis of the ways that providers learn about security incidents and spam trends.
- **Europe** needs to establish a warning mechanism to identify and address emerging threats.

4 Defining appropriate security

For a long time, a commonly accepted goal for information security was to bring it to the highest possible level. This is no longer the case. Overly high security measures will be circumvented with justification by business, while it still holds true that cutting budgets for desperately needed measures jeopardises security and puts business at risk. Moreover, security measures often conflict with the privacy rights of citizens. Striking the right balance and giving providers enough information to make an adequate decision is the main objective today.

4.1 State of the art and cost of implementation

Information regarding what is possible, what is affordable and what is appropriate can come from a variety of sources. No source is perfect, hence it depends on how much one trusts the data, and the guidance that a particular entity compiled. Of course the authority and reach of that entity also plays a role.

Facts and Observations

- Most providers **simply follow 'industry best practice'**. Around half of providers follow international standards. National legislation and advice from the national computer security organisation or from the NRA play a smaller role. (ENISA Survey 2006)
- About half of providers perform an internal risk assessment, but few use a defined **risk management process** or a service level agreement. (ENISA Survey 2006)
- Many providers offer spam filtering **free-of-charge**. (ENISA Survey 2006)
- **Costs for running hotlines** are already very high, and taking security-related calls is an additional burden for providers. (MAAWG Conference)
- Several industry surveys have **reported damage figures** (e.g. FBI/CSI report in the US, DTI survey in the UK, AUS/CERT report in Australia, worldwide Deloitte survey), but these figures vary widely and are not comparable. (META Group Research Note #2982)
- Security experts often argue the **usefulness of statistical data on damages** from security breaches. For example, in its 2006 report the Computer Security Institute (CSI) stated that the costs of security incidents are going down, while market analyst Gartner was quick to question such data. There is still no generally accepted measuring scheme. (CSI/Gartner)
- Most people see a benefit in displaying a **trust seal** on a web site, according to a vendor report from 2006. (Goodmail Systems)
- Many domain names are registered only for a few days at no cost (**'domain name kiting'**), enabling click-fraud. On the other hand, domain name dispute resolution is very complex and costly, often involving the World Intellectual Property Organisation (see www.wipo.int), ICANN (see www.icann.org), registrars and law firms. Hence, while many have to share the cost, only few gain benefits from this scam.
- **Forensic investigations** of spam and security incidents are complex (e.g. maintaining the chain of custody) and often feasible only with **expensive** software. They also require a high level of expertise. (MAAWG conference)

Evaluations and Conclusions

- Although various reports on the cost of security measures (and the potential cost of not implementing them) have been published, there is still no common ground for measuring and hence no way to compare different data.
- In a global economy, the state of the art of information security evolves internationally. National initiatives should focus on co-operation rather than on competition about the most appropriate measures.
- A decision as to whether measures are cost effective and appropriate can only be made in a specific context. For example, most providers deemed it appropriate to sponsor spam filtering in an attempt to gain and maintain customer trust – and market share.
- An investment in information security should yield some value, but in many cases providers fail to display and market this value appropriately. A trust seal or a certification helps communicate the trustworthiness of the service and justify the investments made.

- State of the art and cost appropriateness of information security are moving targets. Using a risk management methodology does not directly provide answers but helps lead the way towards solutions and makes the process repeatable.

Advice and Proposals

- Regarding Internet governance discussions, the **European Commission** should be aware of the conflict between easy domain name registration (helping market development) and thorough domain name registration (helping the fight against phishing and spamming).
- **The EU** could encourage research and other projects that support the development and distribution of investigative tools.
- **The EU** could help analyse some aspects of the security policies of European countries in order to improve overall efficiency throughout Europe.
- **ENISA** should continue providing guidance on risk assessment and risk management methodologies (see "Implementation Principles and Inventories for Risk Management/Risk Assessment", June 2006).
- **Member States** should support and promote the use of risk assessment and risk management methodologies to help achieve a better understanding of the cost-benefit relationship of information security.

4.2 Email security versus privacy

A major principle of privacy is to keep personal data stored and transmitted securely. No-one should have access to personally addressed information except the recipient. But what if the recipient does not want to have access to all that information? As with Heisenberg's uncertainty principle which states that the position and momentum of a particle cannot be determined at the same time as arbitrary precision, it is quite impossible to check private emails for security problems without infringing an individual's right to privacy, at least to some extent.

Email security versus privacy

- Conflict exists between ISP obligations and privacy
- Blocking PCs is often deemed illegal
- Article 29 WP opinion mostly allows filtering
- Providers would like more information on spam laws

Facts and Observations

- Nearly two thirds of providers replied that they think **there is a conflict** between the ISPs' obligations to deliver messages/protection of privacy and the use of spam filters that block certain messages. (ENISA Survey 2006)
- The fight against bot-net causes problems for providers, because **blocking** legal and paid-for connections from consumers who are unaware of their infected PCs may violate privacy laws and **is often deemed illegal**.
- The Article 29 Working Party discussed the balance between privacy and security in **Opinion 2/2006 (WP118)**. In short, filtering of email is allowed under certain conditions in the more obvious cases (i.e. protection from viruses and spam), but in other evolving scenarios (e.g. customisation services) further analysis is necessary. (Art.29 WP opinion)
- Allowing subscribers to **opt out** of filtering is **technically challenging**. If filtering is implemented in the backbone at IP level, the provider either allows all email from the filtered network (including spam) or the subscriber cannot receive any email from that network. Specific filtering (i.e. allowing incoming email from a defined address) is only feasible if the user is allowed to see all emails, making it very costly for the provider who has to transfer all emails (including spam) and provide a mechanism for receiving/rejecting specific emails. (MAAWG conference)
- Most providers would like a **workshop** to provide information about the laws and legal problems regarding spam. (ENISA Survey 2006)

Evaluations and Conclusions

- Fighting spam is linked to filtering, but providers have obligations to deliver emails. If they want to help customers there is a constant risk of being in conflict with the law.
- Some providers unofficially told ENISA that they did not want to reply to our questionnaire because questions were embarrassing. They also said that they do filter emails, but they do not want their customers to know it.
- There will always be a conflict between 'protection *of* the individual' (privacy) and 'protection *from* the individual' (security), but there is a range of options to balance the two sides. Before the Article 29 Working Party opinion, the range of legal options was not clear, leading to uncertainties among providers.
- It is not the task of providers to solve legal conflicts; they need clear guidance regarding what is and is not allowed. The Opinion 2/2006, published in February 2006, clarifies legal aspects of filtering significantly. It seems that the Article 29 Working Party document on email screening is not yet well known.

Advice and Proposals

- **Providers** should take into account the Opinion 2/2006 document regarding email screening.
- **ENISA** should promote Opinion 2/2006 views and could organise a workshop on the laws and legal aspects regarding spam.
- **ENISA** should encourage Member States to raise awareness among citizens about blocked PCs, to the effect that a failure to connect to the Internet can be caused by a malware infection on the citizen's PC.
- **The EU** should promote the Opinion 2/2006 document regarding email screening and continue to clarify where filtering of content is allowed, building on this opinion from the Article 29 Working Party.
- **The EU** (namely the Article 29 WP) and providers should enter a dialogue to find a reasonable balance between the cost and the effectiveness of specific filtering for opt-out.

5 Setting standards

Often it is too difficult – or costly – to determine which measures are appropriate. Instead, providers are looking at what others are doing, hoping that the average solution will be both cost efficient and appropriate, from an information security perspective. If something goes wrong, courts and the public will at least attest a best-effort attempt.

5.1 Technical and Organisational Security Measures

Providers have to secure their services but, for the most part, it is up to them to decide the details. Technical security measures can apply to the end-user's device or the network infrastructure hosted at the provider's premises. Organisational measures can have an effect on all parties involved and range from unidirectional information to multi-lateral co-operation.

Technical and organisational security measures

- Most providers use a combination of techniques
- Focus is on protecting own network
- DNSSEC is deployed in Sweden
- Providers quarantine infected computers
- Users act more carelessly at work

Facts and Observations

- Most **providers use a combination** of 3-5 different protection techniques. (ENISA Survey 2006)
- Egress filtering (protecting other networks) is much less used than ingress filtering (**protecting own network**). Most providers offer contact details for email abuse; around 15% of them do not. (ENISA Survey 2006)
- **DNSSEC** is deployed in Sweden, the Russian TLD .RU is signed, and tests have been made by Mexico and the Netherlands. (see www.dnssec.net/news and www.ripe.net/disi/)
- Two thirds of providers **quarantine infected computers**. (ENISA Survey 2006)
- Around half of providers have a Business Contingency process or a Disaster Recovery process (often mandated by corporate governance requirements). However, providers admit that these processes are rarely tested. (ENISA Survey 2006)
- Only half of providers make an effort to **inform subscribers regularly** and in detail, e.g. with written guidance or with regular information via web site, email or physical mail. (ENISA Survey 2006)
- In the United States, 48% of workers who admit they are **more likely** to open suspicious emails or Web links **on their work computers than at home** said it was because they had IT to support them if something bad happened. Germany (39%) and Japan (28%) featured similar results. (Trend Micro study, 2005)
- Many fraudsters are **not concerned about revealing their identity**, because they often live in countries where they do not expect punishment.

Evaluations and Conclusions

- Countermeasures depend on the type of business, the size and the maturity of the provider. They also depend on the type of client on which the provider focuses its activities. Enterprise clients (who often desire some autonomy in their operations) have different requirements from consumers (who often look for the cheapest service). The differentiation between enterprise and consumer clients can be problematic for small enterprises, who often act like consumers (lack of security expertise) but at the same time require business level performance (24x7 connectivity).
- Since many providers depend on customer complaints to become aware of security problems, it follows that most providers offer contact details.
- Providers still do not take training and awareness-raising serious enough and rarely offer courses. One might argue that it is not the role of an infrastructure provider to do so, even though they are in a good position for such activity, given that they have existing relationships with large numbers of Internet users. They would also benefit from having educated users, mitigating the risk of malicious activity from those users.
- Alternatively, the government could be in charge. Examples in some countries have proved that eCommerce benefits when users learn how to use new technology (e.g. introduction of the eID card in Belgium).
- The implementation of DNSSEC in a country is a complex process, and overall DNSSEC penetration is low.

Advice and Proposals

- **ENISA** – in co-operation with the community of providers, should establish a platform for information exchange about measures to secure electronic communications.
- **The EU and ENISA** should promote specific measures such as quarantining of computers (in compliance with privacy legislation), the availability of contact details for security issues and email abuse, filtering and DNSSEC.
- Consumers need better information and training on specific security issues. This could best be provided and would have the broadest reach with **public-private partnerships** between government entities and providers.

5.2 Measures to fight spam

Originally, spam was considered a mere nuisance and not a security issue. However, a changing landscape of threats (sometimes called 'threatscape') makes one question this assumption, as phishing attacks, spyware and botnets (also called crimeware) spread via email and are often indistinguishable from ordinary spam. Spamming in telephony (SPIT) and instant messaging (SPIM) also add complexity to the threatscape.

Measures to fight spam

- Many countermeasures are of a legal nature
- Anti-spam laws are in place in the EU
- Providers are worried about law suits from spammers
- Providers reject direct SMTP
- Statistical information varies
- OECD anti-spam toolkit published
- Several codes of conduct for providers exist

Facts and Observations

- Most measures that providers take to prevent subscribers from sending spam are **of legal nature** such as 'forbid spamming in Terms and Conditions' and 'inform subscribers about the legal consequences of spamming'. The technique most often used to limit spam in received email is blacklisting. (ENISA Survey 2006)
- Almost all EU countries have **anti-spam laws**. However, on a worldwide basis, only 23% of countries have anti-spam legislation enacted; 64% of the countries do not have such laws. (ITU Survey on Anti-Spam legislation worldwide)
- Sometimes providers are **afraid of law suits from spammers** when blocking them. In some developing countries, (anti-spam) law enforcement is seen as difficult, because such countries do not have sufficient investigative powers. (MAAWG conference)
- In nine countries in Europe, **fines were imposed** on spammers ranging from around one thousand Euros up to tens of thousands of Euros (with two exceptions of very low fines). (CNSA)
- Some providers admit that some of their **customers are spammers**. (ENISA Survey 2006)
- Spam statistics from filtering vendors vary widely and change quickly. Often there are only a few EU Member States on the list of sending countries (e.g. www.Spamhaus.org , 21.6.2006, only the UK in position #8, accounting for 3% of spam) and more on the list of spam receiving countries (e.g. four EU countries suffer from 21% of the world's spam, according to TrendMicro, June 2006). In all cases, the US is at the top of the list.

- 25% of **providers reject direct SMTP** connections. The number is increasing as more and more providers decide to 'manage' port 25. Very many providers offer spam filtering free-of-charge on their network, some offer it for a fee, around 20% do not offer any filtering (either with or without a fee). Canadian providers have also successfully used this method to limit spam.
- In 2006, the OECD published the **OECD Anti-Spam toolkit**. It recommends measures in the areas of regulation, enforcement, industry-driven initiative, technologies, education and awareness, co-operative partnership, spam measurement and global co-operation. (OECD Anti-Spam toolkit)
- The joint BIAC-MAAWG (as part of the OECD toolkit), Australia, Finland and Italy (as well as others) have developed **codes of conduct** for providers to fight spam.
- While there have been **initiatives on Whitelisting** for direct email marketing (e.g. the Certified Sender Alliances, initiated by eco in Germany), most email marketers deal with it on a case-by-case basis.
- **Sender authentication techniques** like SIDF and DKIM associate an IP address or a message with a domain name. Although these mechanisms are flawed (spammers use these techniques as well to authenticate their emails), they are part of the solution, and can be complemented with reputation schemes. Sender authentication has already achieved some deployment; in particular large numbers of email senders can be covered by publishing authentication records for high profile domains such as eBay, Yahoo, Hotmail, Gmail, PayPal. When such companies request their users to disregard all emails from their domain that are not signed, this will increase pressure on other companies to also implement sender authentication. (MAAWG conference)
- The EU initiated the Contact Network of Spam Authorities (**CNSA**), bringing together DPAs and NRAs, depending on the country. The CNSA shares information on emerging problems, reporting of spam and prosecution of spam cases. 21 countries have signed up so far. The CNSA is similar to the London Action Plan (LAP), the worldwide initiative led by the UK/US. CNSA and LAP operate closely together.
- There are several **initiatives for collecting data on spam**. 'Spotspam' is an initiative by the German eCommerce association, 'eco', in combination with the Polish NASK, funded by the EU. 'Signal Spam' is a similar project in France, supported by several French ministries. A Memorandum of Understanding between the two initiatives has been signed recently. Digital Phishnet is an initiative in the United States.
- In some countries, **reporting of spam is burdensome**, e.g. different authorities are responsible for different types of spam or complaints are only possible via ordinary mail. On the other hand, in the Netherlands reporting of spam has been made easy with an online form and consequently the authorities receive a large number of reports. (CNSA)
- Consumers' reporting of spam is a problem. Even if reporting is made easy, deleting spam is always easier. A **decrease** in reported spam **does not mean less spam**. (CNSA)

Evaluations and Conclusions

- Europe suffers more than average from spam and is less often the origin of spam. However, it might not stay this way. Spammers increasingly use bot-nets for sending spam from European countries. These are installed on consumer PCs with always-on broadband connections.
- The situation of spam is similar to the situation of firewalls in the early days. Then, the first approach of firewalls was to block all malicious traffic, similar to blacklisting of spammers. This works, as long as the type and volume of malicious traffic is understood and controllable. Later, the strategy for firewalls changed from default-allow to default-deny, which is similar to whitelist filtering and the authentication of email.
- Detailed technical and organisational guidance on fighting spam is available.
- From a legal perspective, spam originating in Europe is not the problem; it is the lack of anti-spam laws and their enforcement outside of Europe. Within Europe, the legal conflict between confidentiality of communications (privacy) and filtering of communication (security) is more relevant.
- It should be noted that spam is not simply a problem for ISPs. Rather it is a whole ecosystem consisting of big and small connectivity providers, hosters for applications and platforms, DNS, email and other service providers. Technical and legal changes affect the system as a whole.

Advice and Proposals

- **Providers** should focus on driving interoperability and standardisation, in particular of sender authentication mechanisms.
- **Providers** should manage SMTP connections via port 25.
- **Member States** should help educate end-users about spam problems and solutions. This could be done at Member State level, linked to the i2010 initiative and eAdministration.
- Awareness campaigns by **Member States** should also stress that reporting of spam does have an impact on the fight against spam.
- **ENISA** should promote the use of 'Spotspam' and related projects.
- Given the number of best practice guides available, **ENISA** will only summarise best practice and otherwise refer to existing guides.

6 Appendix

6.1 Terms and definitions

Blacklist	A blacklist is an access control mechanism that means *allow everybody, except members of the blacklist*. Source: Wikipedia
Content Filtering	Content filtering is the most commonly used group of methods to filter for security problems (e.g. viruses). Content filters act either on the content, the information contained in the mail body, or on the mail headers (like 'Subject:') to either classify, accept or reject a mail. Source: Wikipedia/ENISA
DKIM	Domain Keys Identified Mail (DKIM) provides a method for validating an identity that is associated with a message, during the time it is transferred over the Internet. That identity then can be held accountable for the message. Source: http://mipassoc.org/dkim/
DNSSEC	DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System (DNS) used on Internet Protocol networks. It is a set of extensions to DNS which provide origin authentication of DNS data, data integrity and authenticated denial of existence (i.e. authenticated non-existence reply). DNSSEC was designed to protect the Internet from certain attacks such as DNS cache poisoning. All answers in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server. Source: Wikipedia, based on RFC 4033-4035
Electronic communications network	Electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting and cable television networks, irrespective of the type of information conveyed. Source: EU Directive 2002/21/EC
Electronic communications service	Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. Source: EU Directive 2002/21/EC
Measures	Information security measures to limit the impact of spam and other malware and to secure electronic communications services. Source: ENISA's own definition
Opt-in	Allowing unsolicited communication for purposes of direct marketing only with the consent of the subscriber. Source: ENISA's own definition
Opt-out	Allowing unsolicited communication for purposes of direct marketing unless the subscriber expressed the wish to not receive these communications. Source: ENISA's own definition
Providers	Providers of electronic communications networks and services such as ISPs (Internet Service Providers), telecommunication companies, hosting and similar service providers. Source: ENISA's own definition
Quarantining a computer	Quarantining a computer means isolating a computer into a special network until it has reached a certain security level. Updates for anti-virus signature files or software patches are made available for installation. Source: ENISA's own definition
Sender ID	Sender ID validates the origin of email by verifying the IP address of the sender against the purported owner of the sending domain. Source: Microsoft

SIDF	The Sender ID Framework (SIDF) is an email authentication technology protocol combining the Sender Policy Framework (SPF) and the Microsoft Sender ID for email into a single standard. Source: Microsoft
Sender Policy Framework (SPF)	Sender Policy Framework (SPF) is an extension to Simple Mail Transfer Protocol (SMTP), the standard Internet protocol for transmitting email. Source: Wikipedia
Whitelist	A whitelist is an access control mechanism which means *allow nobody, except members of the whitelist.* Source: Wikipedia
Zombies	A zombie is a computer attached to the Internet that has been compromised by a security hacker, a computer virus, or a Trojan horse. Generally, a compromised machine is only one of many in a 'bot-net', and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the vector tends to be unconscious, these computers are metaphorically compared with a zombie. Source: Wikipedia

6.2 List of references

ENISA Survey 2006 – Survey on Industry Measures taken to comply with National Measures implementing Provisions of the Regulatory Framework for Electronic Communications relating to the Security of Services (ENISA/TD/SP/06/0055, February 2006) – www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

OECD Anti-Spam Toolkit – published by the Organisation for Economic Co-operation and Development (OECD), Task Force on Spam – (April 2006) – www.oecd-antispam.org/

Article 29 Working Party – Opinion 2/2006 (WP118) – http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf

Contact Network of Spam Authorities (CNSA) – http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/146&format=HTML&aged=0&language=EN&guiLanguage=en

ITU Survey on Anti-Spam legislation worldwide – www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf

MAAWG conference – www.maawg.org

MAAWG Metrics – www.maawg.org/about/FINAL_1Q2006_Metrics_Report.pdf

APWG Phishing Activity Trends Report (February 2006) – www.antiphishing.org/reports/apwg_report_feb_06.pdf

DTI Report on Security Breaches – www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16

Computer Security Institute and FBI report on Computer Crime and Security Survey – www.gocsi.com/

Gartner comment on CSI report – www.gartner.com/DisplayDocument?doc_cd=141622

META Group Research Note #2982 – www.metagroup.com/us/displayArticle.do?oid=48913

Symantec's Internet Threat Report 3Q2006 – www.symantec.com/enterprise/threatreport/index.jsp

Trend Micro study – End-User Revelations About Risky Online Behavior at Work, published in 2005 – www.trendmicro.com/en/about/news/pr/archive/2005/pr091305.htm

Sandvine – Spam/Trojan Trend Analysis (2004) – www.theregister.co.uk/2004/06/04/trojan_spam_study/

The Economic Consequences of Sharing Security Information – Esther Gal-Or & Anindya Ghose, 2005. Industrial Organisation 0503004, EconWPA – http://ideas.repec.org/p/wpa/wuwpio/0503004.html - 2005

Goodmail Systems – www.goodmailsystems.com/certifiedmail/

6.3 Additional links

Best Practice

- Good Practice for combating Unsolicited Bulk Email – www.ripe.net/docs/spam.html
- MAAWG and APWG Anti-Phishing Best Practice – www.maawg.org/about/publishedDocuments/Anti_Phishing_Best_Practice.pdf
- BIAC and MAAWG Best Practices for ISP – www.oecd-antispam.org/article.php3?id_article=232

Statistics

- MAAWG stats – www.maawg.org/about/FINAL_1Q2006_Metrics_Report.pdf
- Spamhaus – www.spamhaus.org/statistics/countries.lasso
- Trend Micro – www.trendmicro.com/spam-map/default.asp
- Sophos – www.sophos.com/pressoffice/news/articles/2006/07/dirtydozjul06.html

Others

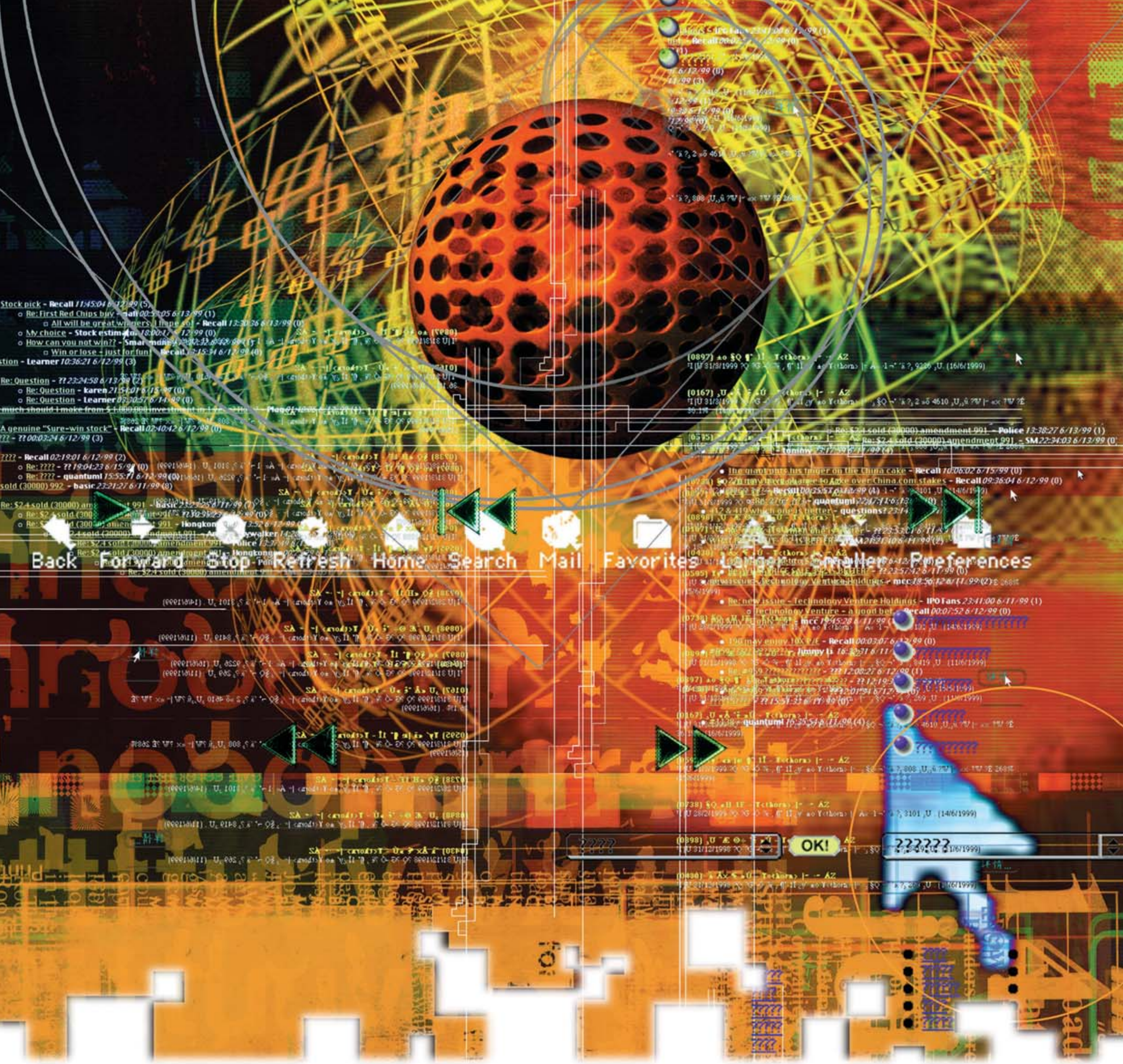
- ITU Cybersecurity Gateway – www.itu.int/cybersecurity/
- Anti-Phishing Working Group (APWG) – www.antiphishing.org/
- Digital PhishNet – www.digitalphishnet.org

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external web sites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.



ENISA – European Network and Information Security Agency
P.O. Box 1309
71001 Heraklion
Crete
Greece

Tel: +30 28 10 39 1280
Fax: +30 28 10 39 1410
Email: info@enisa.europa.eu