Do's:

- Delete - **without opening** - all suspicious subject titles and/or e-mail addresses, often from persons or companies you don't recognize or know directly.
- Be careful when opening **attachments**. These can contain viruses that activate the moment you open them.
- Install a good quality **virus scanner** and **firewall** and keep them up to date. A poorly protected computer can be abused via the internet. In this way you can become the sender of large amounts of spam without even knowing it. High-quality programs are available at your computer store or from your own internet service provider.
- Install a **spam filter** or subscribe to one from your internet service provider.
- Use multiple e-mail addresses and give out your main e-mail address only to trustworthy persons that you know.
- If confidential information is being asked in an e-mail that appears to come from your bank or credit card company (for example your bank account number or login code), **check** by **phone** if this request is truly coming from them, as these kinds of inquiries are highly uncommon.
- If you send e-mail messages to a large number of addresses, use the **BCC**-field **(Blind Carbon Copy)**. In this way the addresses are not visible to others.
- Report spam (coming from your country) at the enforcement authority in your country (see list via OECD-link under 'Legistlation on spam').
- **Encrypt** your e-mail using an encryption program, if you want to be sure that only the addressee gets to know the content. Encrypting your e-mail is similar to sealing an envelope.

Don'ts:

- **Don't buy, don't reply!** Never react to spam, do not buy any product or service advertised and do not try to "unsubscribe" from the list! Purchases reward only the spammer and contribute to the business-case of spamming. Unsubscribing serves only to confirm to the spammer that your email address is still valid. It will consequently appear on more lists and databases.
- Do not react to **false virus reports** (also named **hoax**). These reports encourage you to take measures against a so-called virus. In reality there is no virus, but you will cause damage to your computer. Often you are being asked to send the virus report to as many people as possible. In this way the hoax is being spread like a chain letter, resulting in more damage and inconvenience to more people.
- Be cautious in giving away **confidential information** via e-mail or Internet, like your bank account number, PIN code, password or login data. Always think twice, consider if it is necessary and check whether the party on the other end is really who they claim to be.
- Be careful when revealing your **contact information** on the Internet, like your e-mail address or telephone number. Consider who you are revealing it to and who might have access to it, thereafter.

For more information and questions about spam you can contact:

http://www.oecd.org/sti/spam

http://www.itu.int/osg/spu/spam/background.html

http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/text_en.htm

This brochure is a coproduction of the Netherlands Ministry of Economic Affairs and the OECD. It is a translation of the Dutch spam flyer that is made available in English and French. This brochure can be used in all nations free of rights.

Ministry of Economic Affairs

OECD OCDE

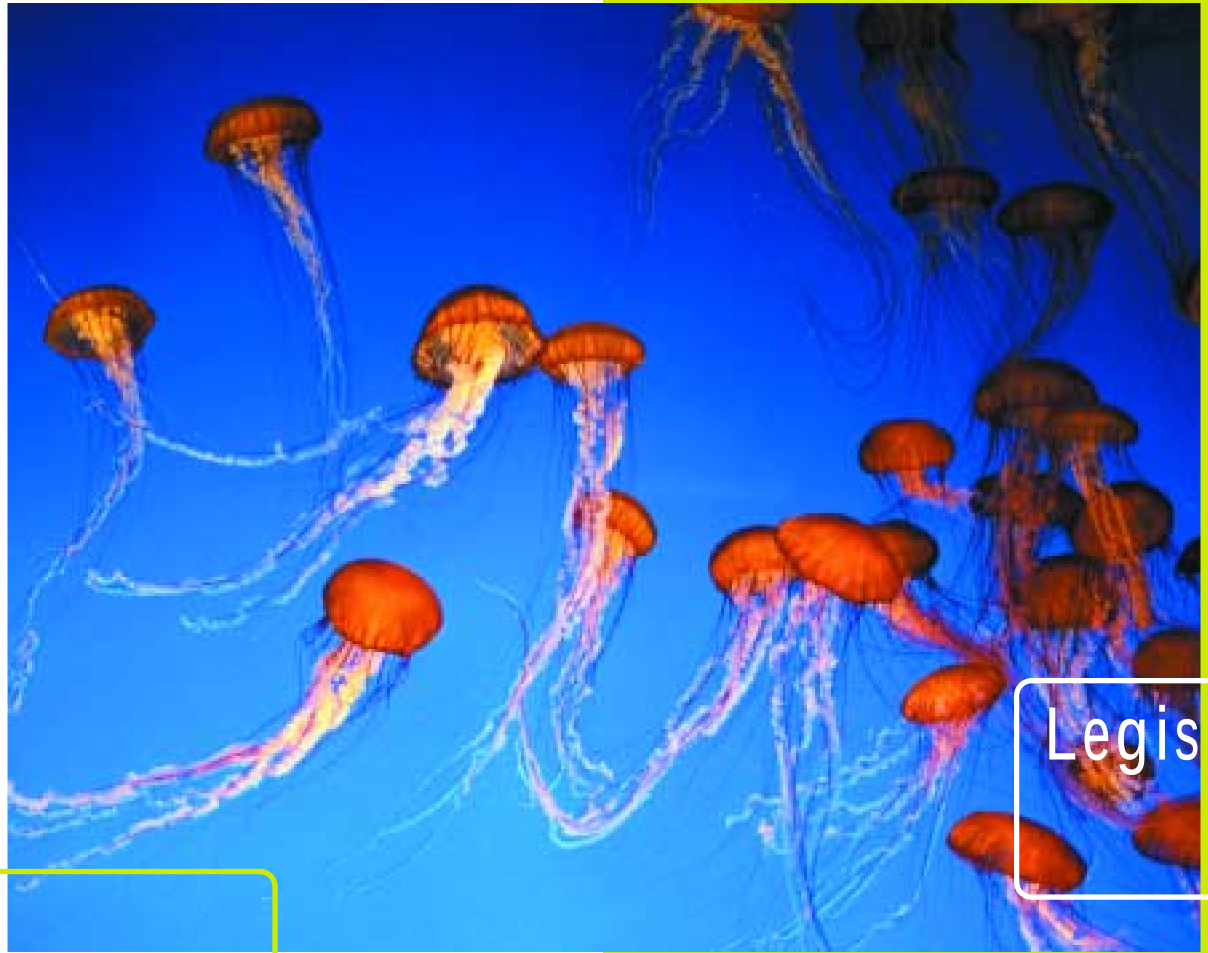
Information Society

Concept and design: Edauw en De Rooij bv, The Netherlands | www.edauw-derooij.nl

SP@M

What to do against unsolicited mail

The benefits that the Internet and mobile technology can provide are without doubt considerable and continue to grow. However, pitfalls do exist and 'Spam' is one such example. Anyone who uses the Internet, who sends e-mail or uses mobile phones will at some point come across the spam phenomenon. But what exactly is spam, where does it come from and above all, what can we do to protect ourselves against it? This brochure gives a short answer to these questions.



What is spam?

Spam is the generic term given to unsolicited and unwanted messages sent to your e-mail account or mobile phone. In other words: electronic junk mail. Invariably it takes the form of an advert and is sent out to vast numbers, sometimes millions, of addresses. The message seeks to convince you to visit a website, maybe browse further, buy or subscribe to a particular product or service.

Worldwide, more than half of all e-mail is spam and many consumers and companies experience inconvenience from it. Spam causes irritation, adds to receiver costs (system capacity) and takes time to remove. Its content can cause damage to your pc's and more worryingly spam is now being more frequently used for criminal purposes. It can be used for the dissemination of computer viruses or the creation of so called zombie-networks - remote computers designed specifically for illegal activities. Another criminal application is *phishing*. This is a type of internet fraud which seeks to persuade you to give away confidential information (PIN code or credit card number). An e-mail message will be disguised as a trustworthy institution such as your bank or credit card company and the fake identity can appear very convincing and reliable.

Legislation on spam

Many governments are trying to combat spam. Several countries have legislation to restrict or ban spam. And where there is legislation, there is also enforcement of the law. The OECD provides a contact list of enforcement bodies in different countries where citizens can complain about spam they've received. This list is to be visited at the OECD website:

www.oecd.org/sti/spam/toolkit

How do I deal with spam?

The measures undertaken by governments and companies are a first step in the right direction of dealing with spam in a more effective manner.

But internet users themselves can also take several measures to avoid spam as far as possible.