# ISP actor

This chapter describes how Internet Service Providers (ISP) are involved in the SPAM issue concerning four distinct topics. First, concrete counter measures that ISPs could use to mitigate SPAM. Second, the distribution of costs and benefits after the counter measure is implemented. Third, what incentives could be to actors to implement the counter measure. Fourth, the role of externalities when counter measures are enacted.

## Concrete counter measures

This subchapter describes concrete counter measures that ISPs could use to mitigate SPAM.

A very stringent but easily implemented counter measure to block SPAM is to block port 25 for all users of an ISP. Mail Transfer Agents (MTA) use the Simple Mail Transfer Protocol (SMTP) over port 25 to receive e-mail. A MTA is a service running on an e-mail server. There is no feasible way to adapt the MTA by using another port because port 25 is hardcoded into the MTA. As such, the whole world needs to adopt using a new port number, which is almost impossible due to the lock-in effect. Moreover, using port 25 for SMTP is a standard defined by Internet Assigned Numbers Authority (Internet Assigned Numbers Authority (IANA), 2016).

However, it is possible to circumvent a port 25 block by an ISP. A user would need an MTA proxy accepting connections on the official port 25 and a user chosen alternative port (for example port 1025). A user can then send and receive e-mail on port 1025 to the proxy MTA which in turn connects to the recipient server on behalf of the original user. Receiving e-mail from an external party would mean querying the MX DNS records from the PC user inside the ISP network. The MX DNS records will point to the MTA proxy for receiving e-mail. When the MTA proxy receives the e-mail from the external party the e-mail is forwarded over port 1025 to the user inside the ISP network. A schematic representation is shown in Figure 1.

The only means that users are left with is using the webmail client of the ISP that can be protected to the ISP’s liking and of course counters sending mass e-mail (e.g. SPAM).



Figure 1 Blocking port 25 for all users of an ISP; but can be circumvented by using proxy

## Distribution of costs and benefits

This subchapter describes the distribution of costs and benefits after the counter measure is implemented.

The scenario to block port 25 would require an ISP to configure firewalls. Such action would mean direct costs due to manual labour of personnel of the ISP. In addition, indirect costs to the ISP are (angry) customers leaving the ISP for alternative ISP’s that do not block port 25.

Costs to ISP users circumventing the port 25 block need to pay an annual fee to a MTA proxy. However, depending on the contract that the ISP has using other Autonomous Systems (AN), as the Internet is a network of networks, this extra traffic could mean extra costs for an ISP due to extra traffic via the MTA proxy. Nevertheless, e-mail traffic comprises only of a small portion of all data traffic on the Internet.

Benefits to ISP’s would be less support questions about malware infections and other SPAM related incidents. In contrast, when a port block would be applied, in the early stage of execution users would call support more why they are not able to use their desktop e-mail clients anymore. However, after this initial period of extra support calls, the number of calls will decline below previous levels.

Benefits to users would be higher productivity, because less time is spent on processing SPAM e-mails (e.g. deleting the e-mails). Moreover, users could also, as an aggregate, gain productivity because malware has to pass the ISP’s stringent security measures and thus the likelihood of infection of users will drop.

## Actor incentive

This subchapter describes what incentives could be to actors to implement the counter measure.

Incentives for ISP’s to block port 25 should to be economical loss and damage of reputation. For example, scanning e-mail activities requires an ISP to buy hardware, maintain this hardware and accompanied software by experts which has its costs. In addition, for ISP’s it is economically quite convenient to block port 25 because damages to reputation and the cost of hardware, up-to-date software and experts add to subscription costs to users, severing competition. Furthermore, the reputation of an ISP is at stake when massive amounts of SPAM are sent from their users in their network. IP addresses might end up in a block list like a DNS-based Blackhole List (DNSBL) or Real-time Blackhole List (RBL). As a result other ISPs and other parties such as companies might be inclined to block an entire subnet (i.e. a whole block of IP addresses) which severs connectivity and thus the reputation of an ISP. Blocking port 25 for ISPs is thus incentivised by bad economic- and bad reputation consequences.

Another incentive could be governmental intervention dictating countering SPAM by blocking port 25. Especially from China and India originates a large amount of SPAM. This is mainly due to a lack of controls at the side of ISPs. When ISPs do not see the benefits of blocking port 25 themselves the government may exercise its jurisdictional power. Incentives to force ISPs to block port 25 could be of all kinds, including financial and administrative punishments.

Creating incentives to ISPs could also be organised by non-profit organisations, NGO’s or a group of enthusiast experts. Legal actions could be informing customers of an ISP that the ISP does not care about customer safety or customer productivity loss. The results might be that creating awareness among customers leads to customers changing ISP and in turn leads to an economical loss to the ISP. Moreover, when the loss of customers is massive enough, this incentive will lead to the ISP taking action to listen to its customers and prevent SPAM. In contrast, actions can be illegal like attacks against ISP servers (e.g. DDoS) to force an ISP to act on countering SPAM. This action might be seen as a last resort when ISPs do not care about a SPAM problem that leads to external severed safety and productivity loss.

## Externalities

This subchapter describes the role of externalities when counter measures are enacted.

Externalities due to blocking port 25 by ISP’s could be that SPAM needs to be delivered more intensively through ISP’s that do not block port 25. In such case there is only a shift in delivery channels. Blocking port 25 needs to be, to some regional extent, a cooperative effort. At the borders of these regional sections (for example Europe) extra, collective, measures could be taken to counter SPAM which drastically lowers the cost of SPAM due to not needing to defend against SPAM within the region itself but merely at its borders.

Another externality could be that an ISP gains too much power. When customers start migrating, from ISPs that do not counter SPAM, to ISPs that do counter SPAM a change in power balance might occur. One ISP might gain customers due to favourable SPAM policies. However, this ISP might have poor policies concerning other cyber threat issues. Especially in customer behaviour it is difficult to predict what attitude customers have towards a favoured product or service (e.g. an ISP) and the alternatives (e.g. alternative ISPs) (Yang, 2014). The quality of the service of an ISP might depend on other factors than SPAM that weigh heavier for a customer that is unaware of the ISP contribution of SPAM due to its policies. However, when customers do decide to massively move to another ISP new problems like an emerging monopoly or lower Internet speeds due to a higher saturation of bandwidth might emerge in the ISP network.

# References

Internet Assigned Numbers Authority (IANA). (2016, October 20). *Service Name and Transport Protocol Port Number Registry*. Retrieved October 22, 2016, from iana.org: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Yang, L. W. (2014). Distinctively Different: Exposure to Multiple. *Journal of consumer research, Vol. 40*, 973-992.