## 1 US Companies

## 1.1 Concrete counter measures

US companies can lose up to 10 million dollars spending on lost productivity of their employees (WITHWORTH, 2004). The most obvious countermeasure to be used by companies is a decent spam filter. The effectiveness of spam filters although differ a lot, just like the way it works. If email (for example) is filtered, a difference between legitimate mail and spam is made. Employees doing this by themselves costs a lot of time and money (and irritations probably). The classification of spam, separated by a spam filter, can be divided in four parts (Thorkilssen, 2004): true positive, true negative, false positive and false negative:

|  |  |  |
| --- | --- | --- |
|  | **Classified as spam** | **Classified as no spam** |
| **Spam in reality** | True positive | False negative |
| **No spam in reality** | False positive | True negative |

The spam problem is growing strong, meaning filters are having an increasingly hard time to separate legitimate mail from spam. Using SPF, DCC greylists and statistical filters like Naïve Bayesian is becoming more popular. SPF and DCC greylist focus on providing identification on the SMTP layer.

SPF stands for Sender Policy Framework. The hole in SMTP is that any client can assert any sender address, which is exploited by spammers to forge email ((THORKILSSEN, 200). The SPF tries to close this hole by forcing the connecting client to identify himself by sending domain, making it unable for spammers to use non-existing domains. It makes it easier to identify spam.

DCC greylists are not like blacklists, rejecting mail absolutely, but requires mail from unfamiliar senders to be retransmitted by their ISPs SMTP clients (THORKILSSEN, 2004). Most spam is sent via open proxies or software that do not use normal Mail Transfer Agents (MTA’s). When unfamiliar senders are temporarily rejected, the normal MTAs will repeat transmission, but the spam sent through a proxy will not be retransmitted. DCC is a free software implementation of a greylist.

Naïve Bayesian is a statistical filter, used in most popular spam filtering software. It has proven to be very effective: up to 91.7% was correctly classified (THORKILSSEN, 2004). The idea behind is that email is represented as a vector with attributes, and every attribute represents a word occurring or not. Then the formula looks at words matching with words in a category c. Then the probability is calculated a mail contains spam or not.

Employees of the company will still need some time to check their spambox on mails that are false negative classified, but it will decrease the amount of time and costs a lot if the company invests in a decent spam filter, combining SPF, DCC greylists and statistical filters. The combination has been proven to be quite effective (THORKILSSEN, 2004). Besides that, the probability to be hacked by a virus sent through an email will be reduced.

## 1.2 Distribution of costs and benefits

To invest in a decent spam filter, can cost quite a lot of money. The big question is: what are the clear benefits? According to WITHWORTH, 2004, US companies lost 10 million dollar on lost productivity. Besides that, every year employees waste two working days (more than 1200 minutes) dealing with spam (CALIENDO ET AL.).

Filtering rate can be seen as a measure of performance for spam filters. The false positive classified mails are the mails where employees can lose possibly important information. It can be seen as bugs in the spam filter (THORKILSSEN, 2004). If an employee is forced to go through their spam inbox a few times a day, he might see the true value of a spam filter. It is more annoying than deleting a false negative mail, coming through the filter once in a while. The error cost of a false positive should therefore be assigned a higher value than the false negative (THORKILSSEN, 2004).

Besides this, another study argues the spam filter mechanisms increase further expenses on spam. The real cost-saving effects have been unclear so far. Caliendo, Clement, Papies and Scheel-Kopeinig (2008) argues the cost benefits should not be seen at the level of the entire company, but at the level of the employees. As said before: two working days per employee, that is a lot of money. Costs savings is proven to accumulate to 439 minutes per employee per year (CALIENDO ET AL.).

(CALIENDO ET AL.) also argues, to optimize costs and benefits, companies should use different strategies for different employees. They should use spam filters for users with little knowledge about spam, and thereby reducing costs. If a user is well informed or not very affected by spam, companies should not encourage the use of an expensive filter. Manual inspections appear to be more efficient for this group.

## 1.3 Actor incentive

As mentioned before, companies could reduce ‘lost’ spending on employees going through spam mails. Because the use of a decent spam filter for ingoing email is pure self-interest (not being hacked, keep your employees from unnecessarily time consuming, annoying work), there is certainly an incentive to use spam filters as a countermeasure.

Besides that, a company does not want to be the victim of spam sent out of their own name: so-called joe-jobs. If spammers know a company is weak regarding to spam protection, they might pick that weak company earlier than a company with strong spam policy.

## 1.4 Externalities

*Snapte ik niet helemaal, kan er morgenochtend nog naar kijken of bij de feedbacksessie*

Thorkildssen, H. W. (2004). SPAM—Different approaches to fighting unsolicited commercial email: A survey of spam and spam countermeasures. *Network and System Administration Research Surveys*, *1*, 45-55.

Caliendo, M., Clement, M., Papies, D., & Scheel-Kopeinig, S. (2008). The cost impact of spam filters: Measuring the effect of information system technologies in organizations.

Whitworth, B., & Whitworth, E. (2004). Spam and the social-technical gap.*Computer*, *37*(10), 38-45.

(Caliendo, Clement, Papies, Scheel-Kopeinig, 2008)