

## profilter Anti-Spam FAQ

1. How does it work?
2. Is **profilter** right for me?
3. How do I use the **profilter** service?
4. Are Virus Hoax emails detected by **profilter**?
5. What percentage of the email traffic is classed as spam?
6. How much time is lost through staff dealing with spam?
7. What happens to a spam email?
8. What are public lists?
9. Is there a limit on the number of IP addresses that customers can input to their white and black lists?
10. How big a problem is unsolicited e-mail (spam) in the workplace?
11. What happens if **profilter** blocks a non-spam email?
12. How do I know if a message has been scanned by **profilter**?
13. What is the real cost of spam?
14. Is spam in the work place a greater risk than viruses?
15. What is the technology behind the anti-spam service?

### 1. How does it work?

Basically you redirect your emails to our **profilter** mail gateway by changing your MX record or we can pop them from your mailbox. When we receive your message we pass it through the following passes.

- Black List
- White List
- Header analysis
- Body of the message analysis
- Attachment analysis
- Attachment Virus Scan
- Threat Analysis

After your message has gone through the above process it is either tagged as 'spam' or genuine email ('ham'). Genuine email is then forwarded onto your own mail gateway. Any email recognised as spam will be quarantined, and wait for you to action it using the online management portal.

### 2. Is **profilter** right for me?

If you receive unsolicited junk emails and viruses by email then the answer is yes.

### 3. How do I use the **profilter** service?

That depends on the type of mail service you have.

For SMTP; after you have registered for the service you will need to change the MX record on your Internet domain name to point to **profilter.prolateral.com** when a message is received for your domain name it will go through the **profilter** and then be delivered to your original mail gateway.

For POP3; **profilter** will pull the messages from your existing mailbox and leave the washed email in a prolateral secure mailbox. You then simply change your POP3 settings on your email client to receive your messages from **profilter.prolateral.com** instead of your Internet Service Provider.

### 4. Are Virus Hoax emails detected by **profilter**?

Although hoax virus email doesn't contain a real virus, an anti-virus gateway will not spot it. **profilter** analysis recognises it as spam, and therefore blocks these type of messages.

### 5. What percentage of the email traffic is classed as spam?

This figure is rising dramatically back in 2000 it was estimated that spam made up 10% of all email messages, in 2002 spam had more than doubled to 25% and in 2004 the figure stands today at around 57%.

## 6. How much time is lost through staff dealing with spam?

On average an individual receives 16 spam per day, it is calculated that it takes on average 30 seconds per email to confirm and delete, thus taking 8 min per day per employee, multiply 8 minutes by 235 day per year equals 1880 minutes or 31 hours per year per employee.

That's nearly a full working week deleting unwanted messages

## 7. What happens to a spam email?

Any spam email will automatically be quarantined and wait for you to access it via the **profilter** portal; either to confirm it as spam or, more rarely, rescue it. If you confirm it as spam email, **profilter** uses that information to improve its recognition of spam in the future.

## 8. What are public spam lists?

Public lists contain email (IP) addresses from known spam offenders: companies and individuals who have demonstrated patterns representative of junk emailing or mass-mailing. These lists are made commercially available to companies. Examples of public lists include ORDB and MAPS RBL.

## 9. Is there a limit on the number of IP addresses that customers can input to their white and black lists?

No. There is no limit for the configurable whitelists and blacklists.

## 10. How big a problem is unsolicited e-mail (spam) in the workplace?

A recent survey by Gartner found that 57% of internal business mail is useless – they dubbed this “occupational spam”. The same study revealed that employees spend an average of 47 minutes per day managing email. This in turn leads to loss in productivity. Spam also put unnecessary demand on Internet bandwidth and the email servers.

## 11. What happens if **profilter** blocks a non-spam email?

The message would be in the quarantined area waiting for you to action it. So in this case you would use the **profilter** portal and select the message as 'ham'.

## 12. How do I know if a message has been scanned by **profilter**?

Every message that goes through the **profilter** service will have additional information added to the messages header.

## 13. What is the real cost of spam?

The average wage is estimated at £15 per hour, so on average with 8mins wasted per day on spam it equates to £2 per day per employee. Multiply this by working days of 235 equates to £470 per year per employee.

As you can see this can start to become very expensive very quickly.

## 14. Is spam in the work place a greater risk than viruses?

Unsolicited junk emails are a big nuisance to any business. Every unwanted message causes wasted time dealing with the message incurring costs and wasting company resources. Being able to remove both spam and viruses before they ever reach your network allows email to be used as it was intended.

## 15. What is the technology behind the anti-spam service?

**profilter** uses continually monitored heuristic rules, self learning Bayesian analysis of content and public collaborative relay & blacklist databases. Emails are scanned using these rules (some 5000 plus) which build a view of the probability of the email being spam. If the email achieves more than a trigger score it is classified as spam and action is taken as chosen by the customer.