

The Confirmation Process

What is spam?

Spam is the name given to unsolicited email messages that are sent to people indiscriminately. These messages might also be inappropriate. For example, an email message offering cheap contact lenses might be inappropriate if sent to people with unimpaired vision. A contact lens user could, however, consider the message to be of value, even though it was unsolicited. This example illustrates a major issue with such email; only the recipient of a message can truly decide whether it is spam or not.

Why can't traditional anti-spam filters catch all spam?

Traditional filters check for spam using several techniques. For example:

- **Filters.** The software looks for key words (e.g. XXX, sex, etc.). When a keyword is found the email message is rejected.
- **Compliance checking.** A considerable number of tools used by spammers generate "non-compliant" email messages. These can be identified and ignored.
- **Traffic Anomaly Detection.** Monitoring where email messages come from and go to will help to detect unusual patterns of email that are often associated with mass mailings. Software can be configured to take action when specific limits are reached.

All of these solutions have several problems

- **Maintenance.** Maintaining a word list for filters can become a full time job for the systems administrator.
- **False positives.** A false positive occurs when a normal, legitimate message is incorrectly identified as spam. Filtering on a keyword such as "breast" will catch all discussions on "breast"s including those concerning say, cancer treatment.

What are the benefits of the confirmation process?

The confirmation process included in GMS Anti-spam together with GMS WebMail...

- **Is easy to understand.**
- **Is easy to use.**
- **Saves time.** Removing the need for users to review spam increases the time available to handle legitimate email.
- **Reduces the number of false positives.** Users no longer need to review their inbox when deleting spam. This dramatically reduces the likelihood that they delete legitimate email accidentally.
- **Can be used with any mail client.** The confirmation process can be used irrespective of mailbox access method. If the GMS Webmail server is also configured for POP3/IMAP using, say GMS Mail, then with any POP3 or IMAP4 mail client (e.g. Microsoft Outlook, Microsoft Outlook

Express, Qualcomm's Eudora, etc.) can be used in addition to the GMS Webmail HTTP client.

- **Has low management overhead.** The system administrator does not have to make changes to the system set up for each user. Each user can choose their own individual settings.

What is confirmation?

Confirmation is an additional stage that requires the original sender of a message to take some action when first communicating. This action "verifies" that the sender

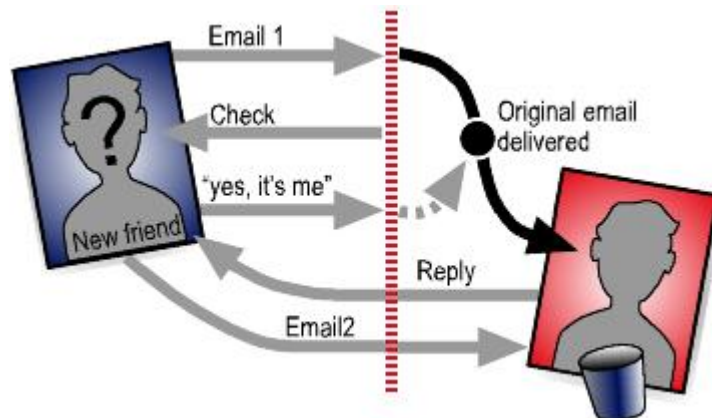
- (a) exists; and
- (b) intended the message to be sent.

Once the sender has returned the verification, the original message is delivered as usual. The recipient can elect to have the sender's email address automatically added to their address book, so the next time a message is received from them the confirmation is not activated. This means that the sender has to go through the process only once.

While messages are waiting confirmation, they are held in a "Quarantine" folder that may be accessed by the recipient at any time. Old messages are removed from the Quarantine folder after a number of days defined by the user.

Example confirmation for Joe, a new correspondent

Martin has just switched on confirmation for the first time. Having previously exchanged email addresses with Joe at a recent conference, Joe now emails him for the first time (email 1 in the diagram opposite). On receipt at Martin's server, Joe's email was diverted into the "Quarantine" folder. Joe is then immediately sent an automatically generated email from Martin's system (check).. It looks like this:



Hi!

Many thanks for your email. Please reply to this message.

Martin

To explain: I have set up an anti-spam filter

which asks for a confirmation from you that you intended to email me. When you reply, the message will be delivered to me as usual and I can read it. You will only have to do this once.

In order for your message to be delivered to martin@dance.org.uk, please reply to this message, leaving the following lines intact.

```
---start  
token:3c89cb835b4a941836b94bd6841f60d5:IoZ7J)Sd  
---end
```

On receipt, Joe simply replies to the message (“yes, it’s me”) and does not have to type anything into the body of the message.

The reply arrives at Martin’s account where the confirmation process identifies the “token” and automatically transfers Joe’s email into Martin’s “InBox”. Martin can now reply to Joe in the usual way (reply, email2, etc.).

There are several choices that Martin has about the way he can use the confirmation process:

- *Checking quarantined email.* At any time, Martin can check the “special” folder called “Quarantine”. This folder contains all the messages waiting for the confirmation response from the sender. After a chosen number of days, messages are removed from the folder automatically. When messages are removed, the sender’s email address can be added to the “block list” so messages from this person are never accepted again.
- *Changing the confirmation message.* Martin can edit the confirmation message so he can provide a personal response in his own language and style.
- *Only confirming addresses once.* Confirmation messages are only sent to those people who do not have an entry in Martin’s address book. Martin could add email addresses to the address book manually (using GMS WebMail’s vCards). To ease management, Martin can decide how which addresses are added automatically. For example, every address Martin emails can be placed into the address book and/or the address of anyone who goes through the confirmation process. This means that the confirmation does not affect those people that Martin already communicates with.

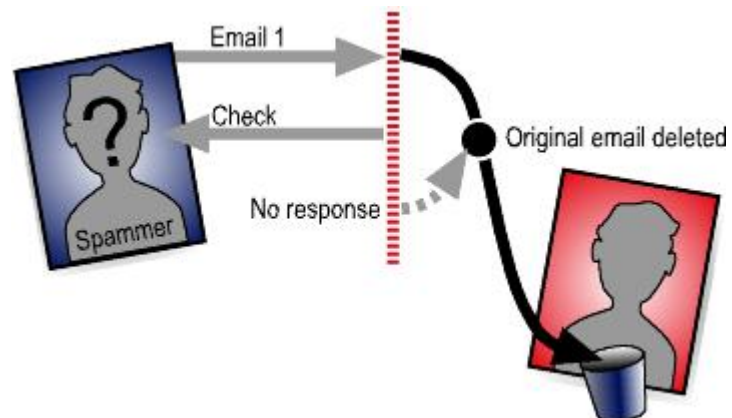
Example confirmation with Sam, the spammer

Sam has just put together a mail shot to 10,000,000 people (email 1 in the diagram below). In the past, Martin’s inbox would have received an email containing yet another “get rich quick” idea. Now, with the confirmation process switched on, he is going to be spared from the hassle.

When Martin’s system receives the message from Sam, it does not find a corresponding address book entry and so sends a confirmation message to

the address in the email message (check). One of two things is now likely to happen, depending upon how Sam sent his spam.

Most spam is sent from accounts that do not exist. In this case, the mail system will return a message (possibly from the “postmaster”) saying that the account is not available. Since the details of this message



do not match Sam’s original message, the confirmation process is activated again and both messages reside in the Quarantine folder. Eventually, the messages will be deleted and the spam never reaches Martin’s inbox.

If Sam sent the message from his own account he will need to personally reply to the message in order for it to be delivered to Martin. For a large number of responses, this is clearly not worth the spammer’s time.

How do I use Confirmation with Microsoft Outlook, Eudora, Pegasus, etc.?

The Confirmation process works on the server by holding messages in a special “Quarantine” folder and then transferring it to the standard “InBox” once a confirmation has been received. If the GMS WebMail server is equipped with a suitable complement, such as GMS Mail, then any mail client that can use POP3 or IMAP4 can subsequently obtain the message in the usual way. Further, those people using an IMAP4 client can also review messages that appear in the Quarantine folder. Each user need only log on to GMS WebMail once to set up their confirmation options and retains the option to access their mailbox via the inbuilt GMS WebMail client at any time.

What about “false positives”?

False positives are only likely to occur if the original sender (in this case Joe) never replies to the confirmation message and even then, only if it is the first ever communication. In this case, Martin is likely to know about the email message through other means (e.g. because they met at the conference) and can simply check the Quarantine folder.

Experience has shown that confirmation actually **reduces the number of false positives**. When users receive a large number of spam messages (e.g. five or ten each day), they tend to simply press the “delete” button to delete anything that looks like spam. This may lead to legitimate messages being deleted carelessly or accidentally.

For example, Martin might have sent a payment for some new software. The company sends the key via email with a subject title of “Amazing Slow Downer for Windows” from an addressee of “Bernadette”. Since Martin doesn’t recognise the name, he simply deletes the email. A couple of weeks later, he rings up to find out what happened to his software!