

Email Defense: Stop Spam and Viruses

Overview

Protecting employees from "bad" email is becoming more and more difficult. Yet, it remains the responsibility of the employer. Although laws have been introduced recently to control spam (unsolicited commercial email), it seems as if the spammers are unaware of them and thus continue operating at full force. There are many problems with spam, including reduced productivity, increased frustration, risk of losing a valid email, and so on. However, one big problem is pornographic and sexually explicit spam. This is a major problem due to sexual harassment laws, and the corresponding obligation of the employer to maintain a workplace that is free from offensive materials. Controlling spam then, is not just a way to keep employees productive; it is a legal obligation of any employer.

Alternatives

Fortunately, there are many alternatives and options available to control spam. Some are free, some are commercial, some work well, and some do not. The purpose of this article is to present various types of solutions available, and then recommend the solution that we have found works the best with the least amount of administrative burden on the company. If you prefer not to read about the technical details, you can skip down to the "Recommended Solution" section.

Email Primer

In order to be able to control spam, we need to first understand, at least at a high level, how email works. Let's track an email that is being sent from a person named "Sender" to a person named "Recipient", as demonstrated in Figure 1 below. First, Sender opens their email program (eg "Outlook") and writes the email. When Sender clicks the Send button, Outlook transmits the email from his computer to an email server (called Server S), which is online 24 hours a day waiting to receive and send email. That email server (Server S) then forwards the email to Recipient's email server (Server R), which is also online 24 hours a day, just waiting to receive email. When Recipient opens their email program (eg - "Outlook"), Outlook asks Server R if there are any messages waiting and if so, Server R sends the email to Recipient's Outlook.

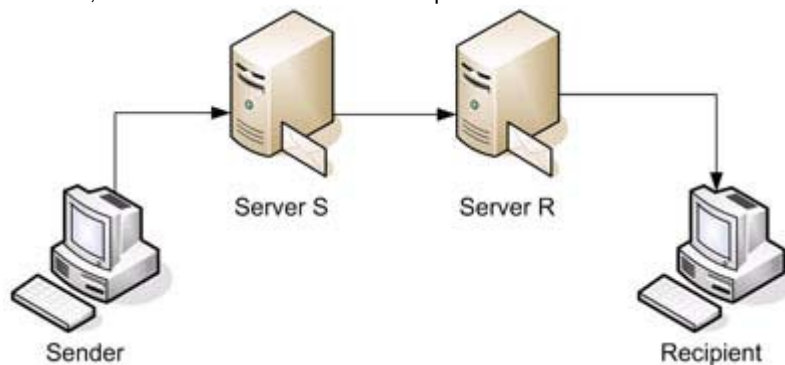
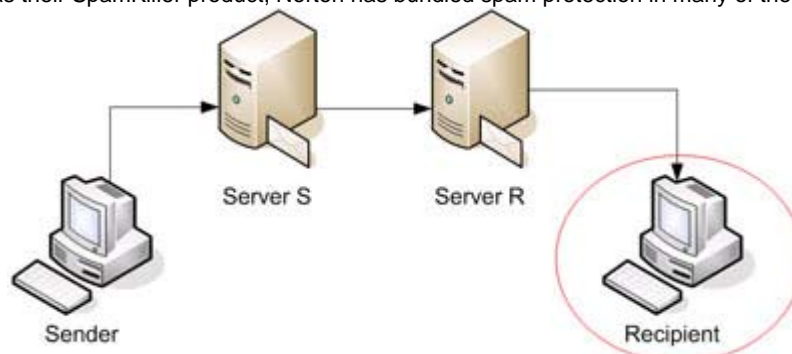


Figure 1

Now, in order to meet our objective of stopping spam, we need to be able to (1) monitor all inbound email (2) attempt to sort out which are spam and which are legitimate and (3) forward the legitimate emails to the recipient. There are 3 places that we can monitor all inbound email: at the recipient's email server (Server R), the recipient's computer, or introduce a new server specifically designed to look for spam. Each approach has advantages and disadvantages.

If we install an anti-spam program on each employee's computer, as shown in Figure 2 below, the disadvantages are that (1) the employee could turn off the anti-spam program (2) an IT administrator needs to install and maintain the program on every computer in the company and (3) an IT administrator needs to monitor individual and varying subscriptions for all employee computers. This approach works well in offices with only one or two people. It is also easy to set up. Microsoft has provided a fairly good "Junk E-mail" box in Outlook 2003. In addition, many of the popular desktop Anti-Virus products now include anti-spam add-ons. For example McAfee has their SpamKiller product, Norton has bundled spam protection in many of their product offerings,



and so on.

Figure 2

In regards to monitoring the inbound email at Server R, as shown in Figure 3 below, many companies do not maintain their own email server, but rather outsource the email hosting service to a 3rd party. So installing an anti-spam program on Server R in many cases is not an option. However, if you do have your own mail server (eg – Microsoft Exchange), there are many Exchange modules that fight spam. In addition, there are stand-al products like Barracuda that work in conjunction with your in-house mail server.

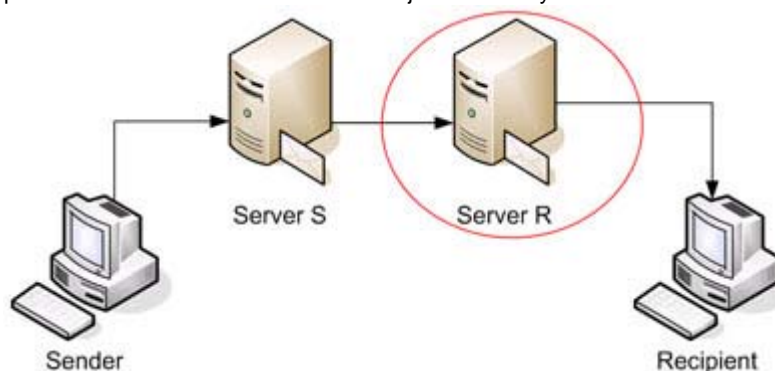


Figure 3

■ Recommended Solution

This brings us to the third option, using a hosted service to filter spam. This model provides the following advantages to the company: (1) no capital expenditures to acquire server hardware (2) no ongoing maintenance by the company (3) easy to implement because there is no software to install at the company. This is the option that, in our experience, is the best.

In essence, we insert a new server in the email flow, as shown in Figure 4 below, whose sole task is to receive inbound email, determine if the email is spam or not, and forward the clean ones to the recipient's mail server.

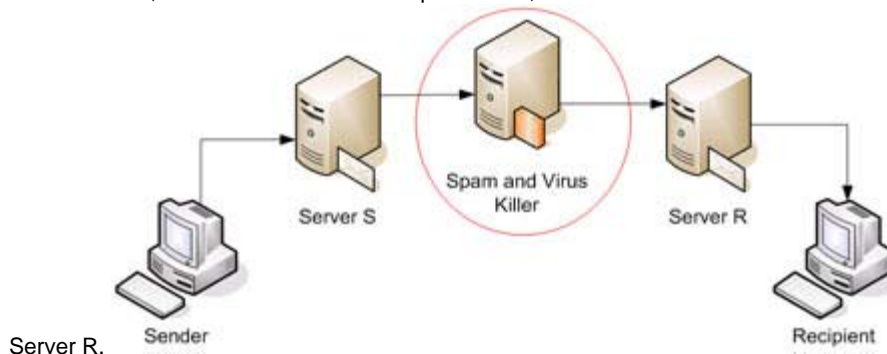


Figure 4

No solution stops 100% of spam, because we are relying on a computer to "read" the email and make a judgment as to its legitimacy. Although the computer does its best, it does not stop 100% of the spam. It has been our experience that this approach generally stops over 90% of spam. There are many great hosted spam filter services out there. A quick Google search will reveal them. For additional information or assistance, do not hesitate to contact us or to visit clickconsulting.com. Regardless of which approach you decide to implement, wish you the best of luck in your fight against spam!