
WHITE PAPER

Spam and Virus Filtering

- September 17, 2003 -

Presented by CyberLynk Network

10125 S. 52nd Street

Franklin, WI 53132

P: 414.858.9335 - F: 414.858.9336

www.cyberlynk.net



WHITE PAPER - Spam and Virus Filtering

Introduction

The purpose of this document is to discuss CyberLynk's spam and virus Filtering Service as a viable option in addressing the security concerns related to spam email and viruses. Since spam email and virus infections continue to be on the increase, the obvious question that begs attention is how to prevent or mitigate receipt and/or infection of spam email and viruses. This document outlines a solution that can prevent a high percentage of compromise to a user's computer and/or network.

Principles of Operation

CyberLynk's filtering service operates automatically to filter unsolicited email and viruses before they are delivered to each users mailbox, thus protecting them and their network from unwanted emails and/or virus infections.

All incoming email is channeled through a bank of dedicated CyberLynk spam and virus servers prior to reaching their final destination. The purpose of the servers is to dissect each and every email and apply a set of dynamic rules to it. If the email fails to pass the rules that have been set up, it is tagged as spam or a virus and the appropriate action is taken. If the email passes, it is sent directly on to the recipient. The CyberLynk filtering service requires no software or hardware on the user's side since the filtering is all server-based. Implementation can be done quickly and effectively.

Processing

Each email that is run through the spam/virus servers is measured against a set of dynamic rules that determine if it is spam and/or contains a virus. The filter is dynamic in that its rule base is continuously updates as new viruses and spam servers are identified.

Filtering - Tests

The filtering process consists of a series of weighted tests (60 plus) that each email is measured against. In addition, customized tests can be created for unique applications. After measurement, every email either passes or fails each specific test. Although an email may fail numerous tests (excluding identification of a virus) it may not be filtered out and tagged as spam. An email is only tagged as spam if the cumulative weight of all failed tests exceeds the pre-determined weight threshold. This is done by assigning a unique weight to each individual test. The weight of each test and the pass/fail threshold is set by the system administrator.

Actions

All valid email not tagged as spam or identified as a virus is sent directly to its intended recipient. The action taken on email that is tagged as spam and/or a virus is determined by the system administrator and can be done on a per-user or per-domain basis. Email identified as carrying a virus is typically deleted immediately and never gets to its destination. Email tagged as spam can be acted upon in many ways. The actions can range from adding the word "spam" in the subject line to deleting the email entirely. Other actions include: sending the spam email to a unique folder; routing the email to a unique address; sending a reply to sender with a "bounce" message; or simply sending the email to a "Hold" (quarantine) directory.

The action applied to failed email can be set and modified at any time. This high degree of flexibility provides users with a filtering solution that can be tailored to their immediate needs and changed as their needs change.

WHITE PAPER - Spam and Virus Filtering

Customer Benefits

The benefits of a filtering service such as CyberLynk's are numerous, and provide a compelling reason to implement the solution. First and foremost is the fact that the service now operates at a 96.4% identification level. CyberLynk's level of identification ranks above the standard and is considered the "Best-of-Breed" by industry experts.

Extended benefits of CyberLynk's filtering service include fast implementation, no staff training, no investment in hardware or software, and it's platform independent. Other benefits include the reduced load on IT staff and internal mail servers, bandwidth savings, and a "Zero" factor for ongoing filter updates. CyberLynk does not need to host the email and the filtering services works with companies that have their email in-house.

ROI (Return-on-investment)

An ROI can be realized in an extremely short period of time. The average company employing 25 people whom process 30 spam emails per day each will loose over \$4,580.00 or 229 hours of production time annually. With the increase in spam emails every day, the loss in production is on the rise. By implementing a filtering service at an average cost of \$45.00 monthly, the ROI period is less then two weeks and the average company can expect to recover \$4,000.00 or 200 plus hours in lost productivity. When reviewing the ROI for virus protection, it is safe to say that any precautionary measures taken prior to an infection can lead to an immediate savings. The cost of not protecting against viruses can be enormous and in some cases can lead to the dissolution of a business.

Conclusion

Whether you use a third party filtering service provider or not, it is important to understand the role that these service providers play in the market. With the increase of spam email and the rise of viruses, companies can no longer rely on internal personnel to provide the necessary preventative measures. Companies that specialize in spam and virus filtering should be employed. They have done the research and have the resources to continually provide the necessary, up-to-date protection that is needed in our ever-changing technology environment.