

## Email / Accountability: A must-have in today's business climate.

**Trusted relationships form the foundation of business which more than ever relies on computers and phones.**

Many of the parties to today's transactions never actually meet face to face. Still they must collaborate, negotiate, and confide in each other across borders and oceans.

Pew Internet & American Life Project has analyzed business email users and found that 62% could be considered "networked workers" who use the Internet or email at their workplace. Fifty percent of corporate employees are in constant touch with their email. Four out of five workers say these technologies have improved their productivity.<sup>1</sup>

Email helps some people avoid awkward initial conversations. For others, it's a convenient way to reach a large audience. [Each day, up to 150 billion unsolicited emails, known as "spam," are sent to individuals and businesses.](#)<sup>2</sup>

TCIM Services, a national call-center company based in Delaware, receives over 27,000 emails each day. CIO Scott von Kleeck says that 150-200 are flagged as spam, but they give users the chance to make the decision. This year, it will mean around 50,000 spam messages to just one company.

Email expert Dan Wallace says that the economics of spam are irresistible to the spammers. "An investment of as little as \$15,000 enables a spammer to send out several million messages a day. There is virtually no variable cost."<sup>3</sup>

The spammer's game is to hope that some of those messages will make it into recipients' inboxes, and that a tiny fraction of those recipients will conduct the desired transaction. Because the spammer's costs are so low, even a tiny response rate is profitable – which is, of course, why spam exists.

Most email users have always believed they can identify spam. In 2003, almost two out of three people told Pew researchers that they "know it right away" (when they see it). Just over two-thirds of emailers said they almost never unintentionally open an email message without realizing it was spam. About a quarter said they do that once in a while, and only 5% say they do it often.<sup>4</sup>

# TDN White Paper

**Spam filters** Users increasingly apply filters to keep spam out of their in-boxes. In 2007, 71% of email users said they use filters provided by their email providers or employers, which was 6% more than two years before. Rudimentary filters categorize some email as spam and drop it into a spam folder. If they made the wrong guess, it is called a “false positive.”

Just over half of email users let it go at that. Some 51% say they check their spam folders at least once in a while. But 46% say they check it almost never or not at all.<sup>5</sup>

But these users are vulnerable to the possibility lost business – and the certainty of wasted time. According to Ferris Research, recovering a genuine email from a spam folder costs an average of \$3.50 of that employee’s time. If you don’t experience many false positives, this may seem insignificant. But in a company of 500 people who have to extract just two emails per month from their spam folder, it amounts to \$42,000.<sup>6</sup>

Says IT expert John Edwards: “Legitimate messages that never reach their intended recipients can easily lead to confusion, anger, wasted time, bruised feelings, missed deadlines and, most importantly, incomplete business transactions.” Accountants and attorneys have been sued for not checking, reading and using important information that was sent via email because of the adverse consequences. Coveted and often rare inquiries from investors, venture capitalists and private equity firms have also been lost.

Some businesses such as mortgage and banking, are particularly vulnerable to false positives since so many spam messages relate to mortgage-and financial-related schemes. Yet any company that uses rudimentary anti-spam technology can expect that at least some legitimate messages will be incorrectly identified as spam.<sup>7</sup>

Spam filters often snare companies legitimately using email to market their products or services. In some cases, these offers may well represent relevant value propositions to their targets. Missing a critical opportunity to improve your supply chain, for example, may harm your competitive advantage. In fact, in a recession business might depend on the new ideas and fresh thinking that inspire innovation.

## **Three tiers of email accountability**

Accountability is not so much about eliminating any and all suspected spam. It means that all email communications must be accurately handled, with zero negative consequences. Most companies have a rudimentary filter that does not provide complete accountability but eliminates the pain that comes from a deluge of spam. According to a major research initiative by CIO Executive Council and Turner DeVaughn Network, 49.4% of CIOs and senior IT staff used “rules-based filters,” while 19.9% use “permission-based filters.”<sup>8</sup>

# TDN White Paper

**Rules Tier:** Most anti-spam programs filter mail using algorithms and heuristics which look at a combination of the content of the message and the server it came from. These filtering systems have two things in common. First, all of them represent efforts to avoid asking, and thus to guess at the answers to, the questions – “Who are you and what do you want?” Second, they don’t work that well, typically topping out at about 85% accuracy, and are prone to allowing spam and discarding legitimate mail. They also degrade rapidly over time as spammers figure out how to beat them.

## *Rules-based spam filters*

There are a number of tools available that use rules to determine whether an email should be allowed into your inbox. [Rule-based systems examine all incoming email looking for patterns that indicate that the email is junk.](#) For example, if the sequence ‘\$\$\$’ is seen at the beginning of a Subject line, the message is probably spam. Still, rules-based systems have many drawbacks and require time to manage those rules.

These systems have three primary limitations:

- They allow some junk mail to go through because there’s no rule that fits a particular message.
- They block some messages that should be allowed to go through because something in a legitimate message matched a rule.
- They require constant upgrading because as soon as a marketer is labeled a spammer, the marketer will find ways to start again.

These limitations have caused many IT professionals to look to more advanced technologies to eliminate false-positives.

**Permission Tier:** In an identity-driven challenge/response world, email marketers will quickly figure out that only legitimate marketing mail (including a real subject line and a valid return address) has any hope of getting through, and then only to people who are actually interested in what is being offered. Everything else will just bounce off. This will completely change the economics of spamming.

## *Permission-based challenge/response filters*

According to the Walt Mossberg of *The Wall Street Journal*, “the best thing to do is to employ a program such as ChoiceMail, which stops the spammers cold.”<sup>9</sup>

DigiPortal’s ChoiceMail is a permission-based spam filter which is 100% immune to false positives. [Mail from senders whom administrators or recipients have not approved is held in a quarantine folder while challenge messages are issued to the senders.](#) For an email marketer to have any hope of reaching their target, he must do three things:

1. Use a legitimate subject line so that if the recipient happens to look in the quarantine folder, and if he happens to be selling something the recipient is interested in, the recipient can tell from the subject line what that might be.

# TDN White Paper

2. Use a legitimate return address because otherwise he will not get the challenge message.
3. Employ a real person to reply to the challenge because the verification process requires human intervention.

Mail not meeting these requirements gets thrown away automatically. It does not get into an inbox.<sup>9</sup>

The “challenge/response” part of this software model is controversial. A portion of the technology community believes that sending out challenge messages is wrong. The objections appear to be driven in part by a belief that it is somehow wrong for senders to be asked to identify themselves. IT consultants and spammers prefer the status quo, in that the economics of the current system are favorable to many of them.<sup>10</sup>

Some ISPs have also expressed concern that large-scale adoption of permission-based systems would flood them with additional email traffic. The major ISPs are flooded with unwanted email now, both because their subscribers are high-value spam targets and because their mail server addresses are frequently hijacked by spammers. They spend heavily on filtering systems, as well as people and infrastructure to deal with all of this unwanted mail.

These concerns can be overcome if the economic advantages are shifted to a new business model by the filtering system. ChoiceMail by DigiPortal is the premier product on the market today. CNET Product Reviews wrote that it is the “only anti-spam program rated CNET 5 Stars.”<sup>11</sup>

It works as a whole system with a vendor screening portal. IT consultants, marketers, spammers and ISPs already embrace permission-based filters when they can sell more products and services with the most advanced systems.

## *Relevance Tier: Vendor Screening and Gap Analysis*

Once a spammer receives a challenge message, they can respond by acknowledging that they are a vendor and would like to have the buyer consider their value proposition. This requires an additional step.

The most advanced system invites sellers to describe their value proposition in a way that is relevant to buyers. Rather than simply getting dumped into an inbox with a bunch of spammers, their value proposition is featured in a detailed report for the intended buyer. The buyer then provides feedback on those vendors considered most promising. This feedback loop offers significant intelligence to the vendors and assures prospective buyers that they are getting the most relevant and compelling solution.

The reality is that only one out of every ten vendors and marketers has a value proposition of real substance, and what they offer is never as relevant or compelling to some targets as they may be to others. Technology that enables feedback loops will improve the odds, however.

# TDN White Paper

Turner DeVaughn Network has developed a web-based tools that enables sellers to self-diagnose their value propositions and obtain feedback from prospective buyers. It can reveal gaps, weaknesses and areas for improvement. Either way, it delivers useful analysis as the basis for improving interaction with existing customers and prospects.

**The Value Gap** The single most common error that sellers make is to not really know how their product addresses the needs of their customers. The single benefit of greatest value is often eludes vendor focus. Instead, they turn their focus to a growing list of product features that may actually confuse – even overwhelm – prospective customers. The value gap analysis reveals the effect this error can have on revenue and earnings.

Complex features cause excessive adoption costs. Customers are painfully aware that a decision to acquire a product can, to put it mildly, make life unpleasant for an extended period of time as they have to figure out how to make it work as promised. Moreover, it eats into profits. Bain & Company has found that companies lose up to 35% of their profits to needless complexity of the products they sell.

The biggest disconnect between buyers and sellers is pricing. Sellers often look to their competitors for guidance, which inevitably leads to ruinous price cutting. The legacy is ignorance about how and where vendors can add-value and justify a higher price. McKinsey & Company research has found that every one-percent of increased price based on added-value generates an eight-percent increase in profits.

**Conclusion** Spam is a bad first impression in a sales process that already is unpleasant for buyers. The most successful sellers pay closest attention to the needs of buyers. The result is value for the customer and profits for the seller.

The challenge for many sellers is to extract the necessary feedback from buyers. Sellers struggle to change internal operations, product and pricing to generate significant ROI.

By combining permission-based spam filtering with vendor screening and gap analysis, companies now bombarded with unsolicited messages can have it both ways with complete accountability: control of spam and identification of vendors who offer relevant value.

# TDN White Paper

## Footnotes

1. "Networked Workers," Pew Internet & American Life Project, Mary Madden, Sr. Research Specialist & Sydney Jones, Research Assistant, September 2008
2. Blog, Web of Trust, Fri 08 Aug 2008, <http://www.mywot.com/en/blog/89-150-billion-spam-emails-sent-every-day>
3. "Why Challenge/Response Makes Sense," White Paper by Dan Wallace, Vice President of Marketing and Business Development, DigiPortal Software, Inc.
4. "Spam," Pew Internet & American Life Project, Senior Research Fellow Deborah Fallows, May 2007
5. Ibid (4).
6. "How Spam Filter False Positives Harm Your Business," Internet Beginners Guide, <http://www.netuser.cc/how-spam-filter-false-positives-harm-your-business-2840/>
7. "False Positives Equal Lost Business," IT Security, John Edwards on February 28, 2008, <http://www.itsecurity.com/features/false-positives-022808/>
8. "How CIOs respond to Cold Calls and Unsolicited Email," CIO Executive Council and Turner DeVaughn Network, Survey conducted October-November 2009
9. Technology, Walt Mossberg, *Wall Street Journal*, January 16, 2003
10. "Why Challenge/Response Makes Sense," White Paper by Dan Wallace, Vice President of Marketing and Business Development, DigiPortal Software, Inc.
11. CNET Product Reviews, [www.download.com](http://www.download.com), August 13, 2004

**Contact:** Stan DeVaughn  
Partner  
650-823-7469 c  
[sdevaughn@turnerdevaughn.com](mailto:sdevaughn@turnerdevaughn.com)

Turner DeVaughn Network  
500 Third Street, Suite 245  
San Francisco, CA 94107  
[www.turnerdevaughn.com](http://www.turnerdevaughn.com)  
[www.netvaluebook.com](http://www.netvaluebook.com)  
[www.netvaluegap.com](http://www.netvaluegap.com)