Brockmann & Company

A New Discipline in Email Etiquette

Creating Confidence in Enterprise Email

Peter Brockmann
President and Research Director
peter@brockmann.com
+1-508-904-0171

April 2007

Introduction

Email has been shown to be a powerful Internet service and an accelerator of commerce, productivity, social interactions, news and amusement. Some call it the Internet's 'killer app.'

It has also in recent years, demonstrated its ability to deliver and broadcast computer viruses, worms, fraud, socially engineered deceptions, identity thefts and global confidence schemes. It seems the service's elegant design as a system to just deliver properly formed messages to the addressees requested by the sender has been greatly abused.

Spam is the embodiment of that abuse of the email service and the best definition that I've seen is:

> To spam: to "indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate email messages, especially commercial advertising in mass quantities. Noun: electronic "junk mail." [1]

Spam affects virtually all of the 1.1 billion Internet users every day. Sadly, the typical email inboxes are assaulted with invitations to click here, download that, visit this site, just email your social security and credit card numbers here or there, participate in this nefarious fraud or that one.

For enterprises, where email has been proven to be a very effective mechanism to communicate with all manner of audiences including employees, potential employees, retirees, customers, prospects, former customers, suppliers and coworkers the electronic correspondence service seems to have been losing its potency and business impact, at a time when our economy can least afford it.

This report, the first in a series, reviews email integrity myths and establishes the case for improving the users' email experience.

[1] www.tecrime.com/0gloss.htm.

Myth # 1 – Anti-Spam Filters Work.

False.

Anti-spam email filters don't eliminate spam.

Anti-spam filters work just like the North American automotive industry's product quality (or lack of product quality) initiatives did in the 1970s. In those days, GM, Ford and Chrysler inspected every part of every car at least once and sometimes twice and yet, given the complexity of the vehicles and the wide range of 'tolerances' consumers were assured that every car had at least one defect. It wasn't until the mid 1980s, after Chrysler threatened to dissolve into bankruptcy, that the automotive industry finally got the message – instead of measuring the product quality at assembly, they must measure (and thereby adjust from time to time) the quality of the manufacturing ***process**, **once*** at the source.

So, why don't anti-spam filters work?

Anti-Spam filters can only ever filter out known problems.

Just like the 1970's auto industry, the architecture is the flaw. With email, the architecture of filter implementations forces the scan of message contents of every message to determine context. Filter algorithms compare every message to some profile which may change over time, determined by the analysis of good and bad messages delivered through a process of training.

Filters have become pretty good at discovering identical messages, and even predicting possible spam. Unfortunately, they can't anticipate the full range of criminal intent. They can't determine what phishing story, or content technique is next. They can't determine what's the next hot pharmaceutical or financial fraud scheme.

Q For Future

What are the costs of failed anti-spam measures in terms of productivity? Lost business? User frustration? Have you ever not received an important business email?

For example, today the filtering industry have been making graphic filters all the rage. This is the technique of analyzing the graphics in email to ascertain any filterable messages formatted in the graphic that only humans can read. As quickly as filters adapt to these techniques with optical character recognition software, the spammers implement more complex mechanisms – maybe audio spam is next? And then video spam after that?

This 'arms race' is a losing proposition for email users. There will always be many messages bombarding a user before the filter is trained or updated to filter out that new category of spam. This is why filters are like closing the gate after the horse is out of the barn. The damage from the original spam – virus injection, fraud scheme, phishing – escaped the filter's traps in the first place, and since the gap between the first instance and the filter upgrade can represent thousands or millions of iteration of the technique, the user and the enterprise is therefore poorly served by anti-spam filters.

Taxonomy

***CAN-SPAM Act of 2003** – US federal law regulating email marketing.*

***False positives** – ham that is flagged as spam.*

***Ham** – good email.*

***Fraudsters** – perpetrators of fraud.*

***Phishing** – an elaborate attack combining email, web and fraud that is designed to get identity information - account details or social security numbers.*

***Spam** – unwanted email.*

Anti-Virus filters do eliminate distribution exploits.

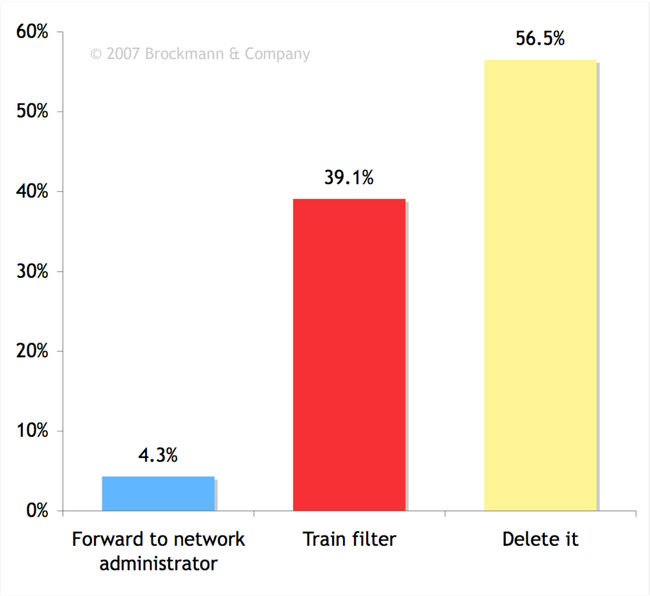
Filtering does have its uses and benefits, just not as a mechanism to eliminate spam. That's because the mechanisms for manipulating Windows are, believe it or not, *fewer and simpler* than the mechanisms for manipulating people. Even the most rudimentary anti-virus filters can detect the most popular methods for infecting PCs - attached executables, executables disguised as other file-types and suspicious zip-format files containing executables.

Like the automotive executives years ago, we need to rethink our approach to email quality. We need to re-establish confidence and integrity into the business of communications. Anti-spam filters clearly can't do it.

Myth # 2 – Nonsense Emails are Harmless.

False.

Figure 1 – Most frequent spam handling techniques.



Many email users get messages with what seems like a random passage from a novel or story. There are no enclosures, no attachments and no links. Besides being a nuisance, how is it that these are harmful?

The goal for these messages is for them to become filter fodder. Spammers send them to users in the hope that they would send them to the spam filter as a sample of spam. Unfortunately, sending these innocuous messages to your spam filter, as 43% of the survey respondents shown in figure 1 typically do, has the effect of de-training it.

Since these messages have many attributes of ham, they work to confuse the filter about what makes spam spam. In the case of these nonsense emails, it is the context that makes them spam. Of course, interpreting context is something that no algorithm can effectively process. Training the filter to consider these type of messages as spam, sadly only has the effect of widening the filter aperture, increasing the rate of false positives and increasing spam that makes it through the filter.

The most appropriate response therefore is to delete the message, as most of our survey respondents report in figure 1.

Myth # 3 – Trapping Good Email is an Acceptable Cost.

False.

This is an excuse for poor anti-spam performance. Email is a business necessity.

Users send all manner of commercial documents through email including orders, contracts, non-disclosure agreements, voicemail, faxmail and appointment confirmations. These business process artifacts move business forward and when the flow of documents is interrupted by the capture and sometimes destruction of legitimate messages by the spam control infrastructure it impacts productivity and reduces user confidence in the business infrastructure, reducing the predictability of the business process itself.

Q For Future

What are the costs of false positives?

Over-zealous filters create false positive incidents which generate insidious, hidden business costs. In the best case, false positives introduce business process delays, effectively slowing the business process down. Users wait until process documents are overdue then they either request a retransmission or go on a search for the missing file if its not too late. Of course, in the worst case, customers place orders via email and you don't know the impact of the false positive because there is no indication that a legitimate message was removed from the stream. Ignorance can be costly.

Some filters even go so far as to create lists of trapped messages so that users can select those they want to further inspect.

Myth # 4 – Some Spam is OK.

False.

This is another excuse for poor anti-spam performance. Just like in the 1970s, the auto industry tried hard to convince us that defective automobiles were a natural part of the industry, yet the Japanese manufacturers introduced vastly superior vehicle quality and thereby earned a growing share of the market, admiration and profits as a result. Toyota, Honda and Nissan did not accept the low standard of some defects. They aggressively managed their manufacturing processes, avoided accepting non-performing product and changed the North American automotive marketplace considerably.

In the case of anti-spam technologies, the identification mechanism is the flaw and *not* the users' fair expectation for zero tolerance.

The Case for Sender Address Verification

There is a better way than to filter.

Leverage the spammer's weakness against them.

The industry has come to the point where it is no longer effective to focus on the content of the message. Instead, it is time to focus on the simpler and more relevant dimension of the *identity* of the email sender.

Consider that a email message header always contain address information such as to, from, reply-to, copy and or blind copy fields. In the fraudulent spam case, the fraudster never attaches their legitimate name and email address. In many cases they spoof a legitimate address that they don't have access to, or they create bogus addresses that facilitate the illusion they are attempting to paint. In either case, they don't have access to the reply-to messages.

Part of this is because they don't want to create an email trail for law enforcement to follow, and part of this is because their email broadcast is a brute force method. For every legitimate email inbox their spam arrives in, there are probably ten that are never delivered and the email management protocol requires the return delivery of a bounced notice. That storm of management information is of no practical use to the spammer.

It is this lack of verified identity that is the fraudster's greatest weakness.

In contrast, email marketers use legitimate email addresses to send from, and often enable processes where the reply-to address is human monitored. It is for these messages that you can with confidence, click the 'unsubscribe' option.

Slow down the interaction with previously unknown correspondents.

A standard email marketing truth is that the most frequent response to an email campaign occurs within minutes and well within a few hours of a message delivery.

Fraudsters exploit this tendency too. They also prefer links over reply email since they are easily redirected to other computers, can involve the download of spyware executables and even complete online forms in furtherance of their fraud. In order to escape detection by law enforcement, they only have these sites up for a few hours.

In the real world, when an unauthenticated person standing on your door step requests your attention, it is a standard social protocol to query their identity, visit objectives, and then assess the consistency of their appearance and body language with that identity and visit objectives, before you invite them into your home. The enterprise email user needs to consistently adopt a similar protocol too.

So delaying a new correspondence for a short time while the sender is being queried is not only polite, but safe.

Conclusion

Sender address verification (SAV) which is also known as challenge-response technology is a valid approach that exploits the weaknesses of spam and is applied automatically only to new correspondents. In its simplest form, the steady state operation of SAV is both elegant and effective. The 'from' field of incoming messages are compared to a directory of verified addresses. Messages from verified correspondents are then scanned for viruses and sent to the users' email inbox. Unverified correspondents are immediately sent an invitation requiring a reply while the message remains in a quarantine folder, before the system can forward the message to the intended recipient.

Spammers never reply. As a result, their messages never get past the quarantine folder of SAV-protected users. In this way, phishing attacks and spam never arrive at the enterprise user inbox.

The technology is only now emerging in credible packaging options, and so its effect on spammer tactics and technology, if any, is not yet clear. In a study of 25,000 enterprise email inboxes, representing some 5,000 organizations conducted earlier in April 2007, no more than 0.1% of these users are protected using this technique. But this is expected to change dramatically by 2008, particularly as the community of SAV users expands. Controlling access to ones' email box through a small 'tax' on the unverified email sender is a simple and effective solution to the scourge that infects so many email users.

SAV Vendors

DigiPortal,
www.digiportal.com,
Hosted service,
enterprise software

Sendio,
www.sendio.com,
ICEbox appliance,
Hardware as a Service

SpamArrest,
www.spamarrest.com,
hosted service

This technique will not eliminate unwanted email completely. But, it will eliminate the fraudulent and downright dangerous attacks, leaving the legally-compliant but annoying marketer to deal with. From there, the unsubscribe option required in CAN-SPAM compliant messages can actually begin to work in the manner that Congress intended.

Surely, the nominal delay and inconvenience of responding to a first correspondence is a worthy consideration to restore confidence in email as an important business process tool.

Brockmann & Company

is a **consulting & advisory** firm serving high tech equipment & application vendors and service providers. Our clients accelerate growth through customer research & thought leadership.

Peter Brockmann, the author of this report, has 20 years experience in process engineering, business development, corporate marketing, product marketing, competitive analysis, marketing communications, branding and Internet marketing. His career has spanned 3Com, Nortel, three startups, middleware companies and application service providers. Particular technologies he has supported or focused on include unified communications, SIP, MPLS, Ethernet, VoIP, PBX, ATM, wireless LANs, VPN, routers, Internet, public key infrastructure and business process routers.

Prior to 2001, Brockmann held various executive, product marketing, and business development positions at Nortel in customer relationship management software, enterprise data products and enterprise telephony businesses. In 1998 he served as an expert witness before the United States Department of Justice and the European Commission during inquiries into Nortel's acquisition of Bay Networks. Brockmann is a Wikipedia contributor, a past-member of the Microsoft Mobile Partners Advisory Council, a recent participant in the Intel Software Strategies Summit and a frequent commentator on technology and business at www.brockmann.com.

Brockmann has an MBA from McMaster University in Hamilton, Canada, a Bachelor of Engineering Science from the University of Western Ontario in London, Canada, and a piano performance degree from the Western Ontario Conservatory of Music in London Canada.

Learn more: www.brockmann.com.