

# The

# EmailXT

# Guide



A guide about EmailXT and how it can solve today's email problems.



# EmailXT

The Official Guide

**(C) 2006 ZOREAN**

v 0.1  
May 22, 2006

## Table of Contents

|   |    |
|---|----|
| Preface.....  | 5  |
| How to read this book.....  | 5  |
| Color formatting.....   | 5  |
| Chapters.....   | 6  |
| Attention Boxes.....  | 6  |
| Chapter 1: About Email.....   | 7  |
| What is email.....  | 7  |
| Email Today : How bad it is?.....                                   | 8  |
| Control of email should remain with the individual.....             | 8  |
| Free speech.....  | 9  |
| Unsolicited communication is free speech.....                       | 9  |
| Wireless.....   | 10 |
| Chapter 2: Spam.....  | 11 |
| Definition of Spam.....   | 11 |
| Why it exists.....  | 12 |
| Impact of spam.....   | 13 |
| Lost productivity.....  | 13 |
| Increased Liability.....  | 14 |
| Downstream liability if spam originates from company computers..... | 14 |
| Subjecting employees to offensive language and images.....          | 14 |
| Loss of confidence in email.....                                    | 15 |
| Spam is growing.....  | 15 |
| Current anti-spam measures.....                                     | 16 |
| Blacklists.....   | 17 |
| Do-not-spam list.....   | 18 |
| Government regulation.....  | 19 |
| CAN-SPAM.....   | 19 |
| Pattern and Bayesian Filters.....                                   | 20 |
| Whitelist filters.....  | 20 |
| Hiding your address.....  | 21 |
| Challenge-Response.....   | 22 |
| Community-based.....  | 23 |
| Impact of current anti-spam measures.....                           | 24 |
| False positives.....  | 24 |
| Important messages being blocked.....                               | 24 |
| Mailing list messages being blocked.....                            | 26 |
| Company products that seem like spam.....                           | 27 |
| Other anti-spam proposals.....                                      | 27 |
| E-stamps.....   | 27 |
| The reasons why e-stamps won't work.....                            | 27 |
| CPU payment systems.....  | 28 |
| Sender authentication schemes.....                                  | 29 |
| Centralized reputation/authentication systems.....                  | 30 |
| Spam and email management in the enterprise.....                    | 31 |

|  |    |
|--|----|
| Checking the quarantine folder.....                      | 31 |
| Managing a whitelist.....                                | 32 |
| Important messages lost or delayed.....                  | 32 |
| The filter vendor exited the market.....                 | 32 |
| Filters that are no longer effective.....                | 33 |
| Chapter 3: Threats by Email.....                         | 34 |
| Phishing.....  | 34 |
| Viruses and worms.....                                   | 35 |
| Spyware.....   | 36 |
| Business Disruption.....                                 | 36 |
| Zombie networks.....                                     | 37 |
| Chapter 4: Security, Accountability and Reliability..... | 38 |
| Security measures.....                                   | 38 |
| Reliability.....   | 39 |
| Archiving & Accountability.....                          | 40 |
| Chapter 5: About EmailXT.....                            | 41 |
| Deployment.....  | 41 |
| Relationships.....                                       | 42 |
| Anti-spam measures.....                                  | 42 |
| Privacy.....   | 43 |
| Ease of use.....   | 43 |
| Virus protection.....                                    | 43 |
| Extensions.....  | 44 |
| Tasks.....   | 44 |
| Calendar.....  | 45 |
| Forms.....   | 45 |
| File Sharing.....  | 45 |
| The Address Book.....                                    | 45 |
| EmailXT and Patents.....                                 | 46 |
| Infinity XT.....   | 46 |
| Chapter 6: Specific Scenarios.....                       | 47 |
| Finance.....   | 47 |
| Marketing.....   | 48 |
| Deliverability.....                                      | 49 |
| Health.....  | 51 |
| Children.....  | 52 |
| E-Commerce.....  | 52 |
| Web mail.....  | 53 |
| Forwarding & Mailing lists.....                          | 54 |

## Preface

The following pages are about email, its current problems, and how EmailXT can solve them.

EmailXT, is a new, rich, client-oriented protocol that aims to evolve email so that it can fulfill the demands of today's most important electronic communication medium: Equality, Privacy, Productivity, Trust and Ease of Use.

**This electronic book is obviously biased towards EmailXT and tries to show its planned capabilities and how they can solve today's and tomorrow's email problems, with many improvements. However, a clean and transparent attitude is taken throughout the entire book.**

**NOTE:** Some EmailXT features described in this book may not yet be developed or deployed at the time of your reading. Please check [www.emailxt.org](http://www.emailxt.org) to see the most updated status report and feature roadmap.

As with any computer protocol, EmailXT is work in progress, and much is still expected to change until its incarnation as a "Version 1.0" protocol.

To learn more about EmailXT and get last-minute information, please visit the public site at [www.emailxt.com](http://www.emailxt.com).

If you want to join the EmailXT community, help on its development, and talk with other EmailXT enthusiasts, go to [www.emailxt.org](http://www.emailxt.org).

To learn more about InfinityXT and download a free copy, please visit [www.infinityxt.com](http://www.infinityxt.com).

## How to read this book

### Color formatting

This book may be too long for those tight-scheduled people that want to skip the prose and just get the hard facts about EmailXT. Taking those readers into consideration, this book presents all EmailXT-related text in blue. Everything else regarding the current email system or anything else is shown in black.

[This text is about EmailXT!](#)

This text is about something else...

## Chapters

This book is divided into six chapters:

The first chapter, entitled "About Email" gives a brief introduction of what email is and how people see it.

The second chapter, named "Spam" needs no introduction. Apart from studying spam and its impact on everyday life, shows how EmailXT can help or fix it. It also contains a limited analysis of other anti-spam proposals.

The third chapter, entitled "Threats by Email" shows the dark side of the Internet, and how EmailXT can help minimize the consequences of the many threats that knock on your computer every day.

The fourth chapter, entitled "Security, Accountability and Reliability" talks about aspects of the current email system that are critical to professional and corporate users of email.

The fifth chapter, entitled "About EmailXT" introduces you to the general aspects of EmailXT, its strengths, and how it integrates with the Internet's current state and people's habits.

The sixth chapter, entitled "Specific Scenarios" uncovers the problems of today's email in many different practical situations, and explains how EmailXT can help or simply fix the problem.

## Attention Boxes

Along the book you will find many text boxes that are specifically formatted according to their contents:

### **FACT:**

The presented facts on the text box have been validated by third-party surveys or studies.

### **NOTE:**

The presented text is noteworthy and should be remembered.

### **TREND:**

The presented figures are predictions from industry experts.

# Chapter 1: About Email

Like the Internet itself, email is an innovation born out of an utopian idealism that has found itself overwhelmed by size and abuse.

When the email system we use today was written in 1977, a single researcher at the University of California at Berkeley had control over how it grew and evolved.

Eric Allman designed Sendmail, a program to make it easier for messages to be sent and received in any computer.

The goal was of course convenience, not security. Security was clearly not a threat at that time. While Allman's invention made it easy for the university academics to reach each other, it also made it easy for those with less honest motives to do the same thing.

Nobody had a chance to change the system before it flooded the entire world. Actually, when people started to identify email's modern weaknesses, it was too late. Now, with millions of email messages running around the globe every minute, the problems threaten to overwhelm the system.

## What is email

Email has grown from a simple tool used by a few academics on the Arpanet to a ubiquitous communications tool. It has evolved from a piece of simple, plain text in an inbox into a rich graphical medium that can be viewed, sorted, signed, encrypted, shared, archived, searched, prioritized, etc.

Email is consistently rated as the most popular and most used application on the Internet. Indeed, some people only use email and do not browse the world wide web at all.

Email is now the preferred primary means of business communication, ahead of all-time favorites like telephone and postal mail. Some statistics:

|     |  |
|-----|--|
| 42% | of business users check their business email while on holiday                |
| 53% | of business users check their email six or more times during the working day |
| 34% | of Internet users check their email continuously throughout the day          |
| 96% | of Internet users' main reason for being online is email                     |

**FACT:** There are approximately 1.1 billion email users worldwide and nearly 1.4 billion active email accounts, as of the end of March 2006.

**TREND:** The email client market is growing and evolving rapidly. It is expected that the email client installed base will increase from about 1.9 billion seats in 2006, to nearly 3.6 billion seats in 2010. That's an average annual growth rate of 18%, and an overall increase of 91% over the next four years.

## **Email Today : How bad it is?**

**FACT:** In May 2005, spam peaked at 93% of all global email. Spam currently accounts for nearly US\$20bn in lost time and expenses globally.

New computer viruses continue to circulate and to present a real danger to individuals' computer systems and files.

Trust on the Internet has been decimated. Many people have abandoned their long-held email addresses, or else adopted over-zealous spam filters. As a result, it has become increasingly difficult and often impossible to find and reach people using the Internet, leading to lost opportunities such as jobs.

We all find it incredibly frustrating not to be able to reach people we know, and we all feel the same indignity when crimes are committed in our names through email identity theft, which can potentially degrade our reputation -- or worse. Indeed, a new trend of emails attempting to 'phish' recipients' banking details is definitively growing, making them 7% of all spam emails already.

**FACT:** Research demonstrates that 1 out of every 500 email messages circulating on the Internet contains confidential information, yet less than 1 percent of corporate and government agency messages are encrypted.

Yes, you got it! Email is sick, very sick. Yet, it is too important today to let it die.

## **Control of email should remain with the individual**

Email control should remain with the individual, actually no person's email should be filtered without their knowledge.

Although it should not be forbidden for ISPs to set email policy for their users, it is better that this could be something users can define and control for themselves. If your ISP filters or limits your email, there should be full disclosure of this to you, and you should have the option to turn it off.

Sites are private property so it is within the ISP rights to specify and negotiate

agreements with their users, and thus to regulate themselves. Indeed, ISPs may view their site-wide email filtering as a feature to be promoted.

This follows the pattern of spam and how to define it: Each person has their own preferences, attitudes, definitions and actions towards email and spam. Why should it be others who define what you can and what you cannot receive?

EmailXT puts the power in the hands of the individual. Default relationship rules are set automatically by EmailXT but the user can freely start and revoke relationships, effectively closing the door to unwanted messages or senders.

## **Free speech**

Email is becoming the premier method of person-to-person communications for dispersed people, overtaking the post office and the telephone in many cases. And this trend will continue. Therefore email deserve the highest levels of protection for freedom of speech. If email fails to be as free as paper mail, significant rights will be lost.

Many people think that because most spam is commercial in nature, and because the commercial speech is less protected under US' 1st amendment, it is the right thing to regulate. Wrong. The supreme court says you can't take that approach. It has been said that if you have a larger problem, of which commercial speech is just one part, you can't go after it just because it is less protected.

## **Unsolicited communication is free speech**

This is one of those hard concepts for some to accept. In a free society, you have the right and ability to get to somebody and talk to them. Or to call them. They are protected by law from being annoyed by such introductions. (They do however have the right to be protected from harassment when these introductions are deliberately repeated.)

This is a good thing. Free society grows from such communications. The problem is that it's being abused by spammers. But the answer is not to just shut the door and lose the vital unsolicited one-to-one communications link in order to stop the current automated bulk mail abuses.

We must work hard to stop spam by the least restrictive methods, protecting ordinary person-to-person communication from being limited.

## Wireless

Wireless email is a means of sending short email messages to mobile devices such as mobile phones, message pagers, or iMode phones.

### Wireless email features

- Improves the timeliness of communication by providing mobile access to email and PIM data.
- Can be offered over a wide range of mobile devices and operating systems.
- Is supported by a wide variety of wireless networks.

As carriers continuously roll-out new wireless email solutions and robust mobile devices, wireless email is evolving from a costly niche service to a mainstream communication method.

**FACT:** The corporate wireless email market installed base will increase from 6.5 million users in 2005, to nearly 123 million users in 2009. This represents an annual average increase of 109%.

EmailXT has one feature that may help you when you are reading your email on the move: A separation between message text and attachments. On devices with limited capacities or storage, you may just download the text part of the email for a quick read. The entire message is kept on the server until you reach your office's computer for a complete download.

## Chapter 2: Spam

The Radicati Group's study, "Messaging and Collaboration Corporate Survey, 2005-2006" concludes that there are still many companies struggling with spam. After several years of frenetic anti-spam product development, many organizations are still not satisfied with the anti-spam solutions they have. Of the four messaging priorities reported (viruses, spyware, spam and email archiving), three are related to security issues. Most surveyed companies (67%) want a solution that does more than just anti-spam, such as anti-virus, regulation compliance, email encryption, and more.

EmailXT comes to fulfill most of current email users' needs by offering an integrated set of capabilities that presently can only be found on separate, non-inter-operable products or services.

### Definition of Spam

To start with, spam is not unsolicited commercial email. If someone in my town heard that I was looking for an old '55 Chevy in good condition, and sent me an email offering to sell me one, I'd be delighted, but still this email would be both commercial and unsolicited.

The marking feature of spam is not that it is unsolicited, but that it is automated. If someone started sending bulk email to support some political or religious cause, for instance, it would be considered as much spam as an email promoting impotence pills.

In some business relationships, you do implicitly solicit certain kinds of email. When you order online, you implicitly ask for a receipt, and a notification when the order ships. I don't mind when a domain registrar sends me email warning that a domain name is about to expire, but when they send me email offering a free guide to "building my B2B web site", that's spam!

Up to now, it was your ISP or your anti-spam software that would decide what message you should read or not. With EmailXT, you decide. Establish relationships with the ones you want to receive email. Reject or revoke the relationships you want to avoid.

Spam is unethical because it disrupts your life and makes you lose your valuable time.

So, why do people report some email as spam, but not other email? It's not just whether the email is unwanted or if it's commercial.

Let's take for instance the case of the emails I usually get from my uncle Bill. When

uncle Bill first got his first Internet account, he loved to send me email. Every joke or chain letter he received, forwarding to me was a sure thing. When he visited a website with funny or otherwise unusual pictures, I'd be the second to know.

So why didn't I click the "Set as spam" button every time I got these messages from my uncle? Although you could say I "opted in" because my cousin gave him my email address, it was sure I didn't want to receive every joke or scheme that had been circulating on the 'net.

The key is the relationship. I didn't report uncle Bill as a spammer, as annoying as his messages could be, because I've had a close relationship with uncle Bill since the beginning of time.

EmailXT enforces the concept of a relationship with varying levels of trust. You may assign higher levels of trust to your family members, while keeping everybody else with a lower level. Contacts with higher trust levels will have access to more of your profile information, as well as other privileges you may grant.

## **Why it exists**

We all hate spam and we like to blame spammers. But anyone who buys products or services from spam email is just as guilty as the spammers for creating the problem. Buying just one product supplies a spammer with enough money to spam another million people.

**FACT:** According to a recently released survey, 11% of computer users have bought something hyped by spam, and 9% have been ripped off by spam scams.

It's no wonder there's spam, and oceans of it.

More than one in five British consumers (22%) has purchased software in response to spam email, a past study by Forrester Research claims.

The poll, jointly conducted by Mirapoint, a message security vendor, and the Radicati Group, a research firm that specializes in email messaging issues, found a surprising fraction of computer users actually open spam, buy its products, and get suckered into its bogus schemes.

Even if they're not purchasing spammed products, nearly 4 in 10 users (39 percent) admitted to clicking on the embedded URLs within spam. More worrying is that 57 percent of those polled who said they clicked on links also said they received more spam after they did.

If people stopped buying products from spam, spam would probably go away.

We have learned that consumers read messages routed to the spam folder. Many

consumers are indeed interested in receiving unsolicited commercial email and making purchases from those messages.

Some people say that the increasing weaponry applied against spam are keeping spammer's messages from reaching their audience. Nothing could be more wrong. You see, those that are buying from spam are normally basic computer users that do not care about spam filters, security updates or best practices. Therefore, spam is indeed reaching its intended audience and spammer revenues are not decreasing. So the flood will continue.

EmailXT will force people out of the shameless spam buying practice. How? As the EmailXT community grows, it will reach spam buyers sooner or later. To reach their correspondents, spam buyers will switch to the EmailXT network in order to communicate with their usual contacts. Since EmailXT is a protected, no-spam medium, these buyers will be kept from buying spam-advertised products, effectively killing spammer's revenue streams.

## **Impact of spam**

### **Lost productivity**

Most of today's organizations have their share of employees who are drowning in spam. Three to five hundred spam messages per day for some employees is not currently uncommon. These employees can come from any level in the organization, from the manager to the receptionist, and everybody in between.

Some of the key problems that result from employees dealing with spam, include the following:

- Extra time spent looking at all email in order to identify and delete spam messages. This is becoming more difficult as spam subjects look more and more like ordinary messages.
- Email quota problems due to spam filling up users' mailboxes. This is especially troublesome for employees on the move, unless they are able to log in every day and clean their inboxes.
- Loss of important business email messages that were accidentally overlooked and deleted. Legitimate messages often get caught in the battle between spammers and filters.
- Phishing messages that look like they originated within the company or from another legitimate source. Most times these scams result in virus infections, security breaches, fraud, and other issues.
- Employees who are lured to visit web sites waste more time and increase the risk of security issues caused by hostile code on web sites.
- Increased computer support costs. Employees who are plagued by spam and

related problems will certainly be calling the IT helpdesk more frequently than employees who receive little or no spam.

For those who have an EmailXT mailbox, lost productivity is a thing of the past. In fact, people may find strange the "quietness" of their mornings at work: No email to delete, no spam folders to check, no phone calling asking whether that message was received or not...

## **Increased Liability**

Most legal departments have not yet addressed issues of corporate liability in connection with spam.

### **Downstream liability if spam originates from company computers**

As most of us already know, spam messages have no return address, so it is difficult to blame those who generate such messages. However, when a company's own email server or one of its client workstations is being used as an email relay, other individuals or companies being targeted by this spam could build a legitimate legal case against the company whose computer is being used to generate or relay spam.

EmailXT email is extremely hard to spoof because an external entity is unable to send spam emails using another company's address. Several levels of protected information would be needed to spoof a message: Relationship codes, encryption keys and CA certificates. It's still possible but it would depend on the spoofed entity's security measures.

### **Subjecting employees to offensive language and images**

An good amount of spam is pornographic in nature, and this obviously means that employees who receive this kind of spam are going to get messages that contain content that may be offensive to them. And not just in the message contents: Spammers are becoming more aggressive and are including suggestive and offensive messages right in the subject line. This could be just annoying to many, but it's also insulting and distressing to others.

In many instances, porn spam is sending some employees "over the top," resulting in animosities and even threats of lawsuits. Organizations that are doing little or nothing to combat spam probably do not have much of a defense in these cases.

Using EmailXT, employees would only receive offensive material through an external address that they specifically authorized to. Therefore, company liability would be greatly reduced or eliminated.

## **Loss of confidence in email**

The diverse types of spam-filtering and blocking tools used by ISPs and other network operators, and the resulting cyclical battles between spammers and spam blockers, produced some unwanted results.

Spam is eroding people's confidence in email as the main form of business communication if it gets to the point where filters get so widespread and aggressive that legitimate mail is lost regularly.

Legitimate commercial email, as well as legitimate non-commercial or personal email, are now increasingly being blocked by filters, sometimes without the knowledge of either the senders or the intended recipients. These filtering techniques, appliances and practices are also contributing to undermine consumer confidence in the reliability of email.

EmailXT increases email reliability since return receipts are mandatory for all regular messages. If your message is not delivered, you will know. If an error occurred, you will know exactly what was the nature of the error.

## **Spam is growing**

Spam is increasingly consuming network resources, CPU resources, disk and network buffers, disk space, everything. If your email server is slow, imagine how much faster it would run if you could eliminate nearly 75 percent of all incoming traffic. On the other hand, if your email server is able to keep up with the torrent of garbage, it's because you have a system that is larger than it should have been necessary.

**FACT:** Current worldwide email traffic per day is about 171 billion messages, of which 71 percent are spam. As of the end of 2005, worldwide email traffic per day was about 135 billion messages, of which 67 percent were spam.

Everybody is in this situation: Either they've had to invest more money in email servers to keep up with the growing tide of spam, or else their mail servers would break under the workload. If your organization is so well organized that you have statistics on inbound email volumes over the last years, you can see that the volume is increasing at a rate that significantly outpaces the increase in the number of employees.

EmailXT increases email traffic since there will be additional system messages circulating in the email infrastructure: Relationship requests, challenges and acceptances, return receipts and others. However, as spam and viruses decrease over time, email traffic will actually shrink and the current server dimensioning will remain effective.

## **Current anti-spam measures**

Today's rising spam volumes mean that the many and expensive approaches to stopping junk email simply are not working.

The fact that the industry has failed until now to adopt a solution that all agree is necessary is a lesson in the complex nature of who controls the online world. Big companies have clashed over who should take responsibility for a resource like email, that no one owns. Individual Internet users have accused such companies of being too concerned about their own agendas to be trusted.

More and more often, software pretends to know what's best for you - and then gets it wrong. Spam is making email an increasingly unreliable form of communication, due in part to our reliance on not-smart-enough software filters that many times let junk through and trash legitimate messages.

Because a common definition of spam has not been reached despite many years of study, it is better to define it your way. With EmailXT's relationship-based architecture, you can immediately eliminate all bulk, non-targeted email, while establishing individual controlled relationships with the legitimate senders.

Solutions that engage spammers and anti-spammers in an intellectual race are doomed to fail, and the process to discover this will be slow and expensive. And why? Because spammers are the ones who take the initiative; all those expensive analysts at anti-spammer houses are worthless until a spammer make its next move and then what all the analysts can do is to catch up. All the software to detect and filter spam email and its administration has a cost, as well as the processes to detect spamming IP addresses.

This happens because current anti-spam technology is based on filtering, a context-less, message-by-message analysis. EmailXT does not need filters or periodic updates because all senders are rejected until they "qualify" as a legitimate one.

Some anti-spam companies deploy systems that check the IP addresses of email messages against "reputation" databases of millions of suspect IP addresses.

This approach makes little sense as both legitimate and illegitimate senders will end up on these databases. And this will not be a problem for the spammers; the fact that these databases exist means that the spammers' use of the recorded IP addresses

will be temporary and being on such lists is of little consequence. However, legitimate senders cannot afford to be so dynamic with their IP addresses and once they get on these lists will be a problem for them as their email is blocked and they have to take action to be removed.

Many examples of these database systems exist, and most seem to rely on a matter of trust. However, how do you know if your competitor might simply have submitted your IP addresses as a source of spam?

Presumably, the first indication that your IP address is on such a database is when sent mail stops getting through: legitimate mail gets caught in the net. It's easy for the spammers, of course, because they simply change their IP addresses regularly. But what about the good guy? He's not going to want to change his IP addresses, or maybe even be able to do so, hence he has to work out if he's on a black list and decide what to do about it. Email administrators have no time to inspect the response from any and every the destination server to determine the true nature of the problem.

The end result is that many of the legitimate mail senders have to take steps to bypass the "bad guy lists", so they all finish up taking the same steps as the spammers.

In EmailXT, there is no "bad guy lists". Instead, there is only one "good guys list". Each user has its own and sets its own policies. The default policies set in place by EmailXT are usually enough, but you can fine-tune it.

## **Blacklists**

Blacklist databases go beyond the obvious – such as listing the email addresses of individuals and companies that send spam. They include the IP numbers of computers that may be sending spam, hosting spammer web sites, distributing programs used to send spam, or have an "open" or "insecure" relay.

The real test of any technique for eliminating spam is not how much spam you can stop, but how much spam you can stop without stopping a significant amount of legitimate email. Email return addresses can be forged too easily: Your messages may be mistakenly identified as spam in various ways. Spammers may forge your email address and use it on their messages, or spam may be going through the mail server that handles your email. You may get no indication that your messages are being blocked, and think that recipients are ignoring you, or saying "no" by not answering.

EmailXT messages cannot be forged simply because for each pair of correspondents, a certain amount of secret data must be used to validate the communication. Unless the security of one on them is compromised, there is no way to forge a message.

Simply blocking mail from any server listed on a blacklist, as some ISPs do now, is in effect a clumsy form of filtering - one that generates a large number of false positives, and yet only catches a small percentage of spam. Spammers seem to have little trouble staying a step ahead of blacklists.

Also, some blacklisters blacklist entire ISPs and networks in the hope that other users will push to punish the spammer on the same network. Punishes the innocent in order to get the guilty - never acceptable in a just system.

Blacklists have been around for years. If they worked, we'd know by now. But according to a recent study, one of the best known blacklists, catches only 24% of spam, with 34% false positives. It would take a conscious effort to write a content-based filter with a performance that bad.

Critics charge that blacklists and other self-appointed sheriffs of the Internet have overstepped their bounds, wielding great power without any authority. Like other kinds of vigilantes, anti-spam vigilantes often do more damage than the problem they're fighting. In effect, blacklist services waste most of their ammunition on civilians. The ACLU, the Electronic Frontier Foundation, and Computer Professionals for Social Responsibility (among others) have all condemned the practices of blacklisting groups.

Blacklists only have the power that they do because ISPs are desperate and feel they have no alternative.

With EmailXT, individual users make their own policy: Several levels of mailbox access can be defined and relationships can be established and revoked at any time. There's no need to rely on third-party policies, although a reputation-based system could later be built into EmailXT. This is a topic still under research.

## **Do-not-spam list**

CAN-SPAM legislation in the U.S. required that the FTC (Federal Trade Commission, the government bureau that oversees and regulates commerce) study the feasibility of creating a national Do Not Spam list that would be similar to the Do Not Call list that telemarketers are required to conform with.

However, the FTC has thus far recommended against the creation of a Do Not Spam list. Unlike telemarketers, who are relatively easy to find, spammers send their spam through thousands of open relays and zombified computers. Further, spammers frequently operate — or relay their messages through — overseas connections, which is one means to distance themselves from the long arm of the law.

Thus, it is thought that a Do Not Spam list would actually become a Do Spam list, because spammers are accustomed to operating outside of the law.

Obviously, there is no need for such a list with a system like EmailXT.

## **Government regulation**

Is government regulation of email the answer? Is it something we want to encourage? It's more like a last resort, and we haven't tried all the other resorts. Spam has been around for some years now, a long time in an internet scale, but just a blink of an eye in the world of law.

Even the USA's federal government is limited in what it can do. Spammers can quick and easily move to other countries to continue their activities.

If the "law" is made by you at the receiving end, it doesn't matter where in the world emails are sent. Every message that is not compliant with your locally-set policies will be rejected, rendering spam operations useless. No need to worry about national laws or foreign treaties (or lack of them).

The truth is that the junk fax and phone call laws have been remarkably ineffective. Now the US have at least 23 state spam laws and as far as can be told, apart from a few successful cases, they haven't even dented the problem, just caused friction and legal battles.

The problem here is that it means we are allowing the law to dictate things about the content of our email. One email would be legal and another one would be illegal just based on what the email contains. Isn't this a bad direction to go?

What the law does, if anything, should be based on the manner of sending, not the message.

## **CAN-SPAM**

Those that have been tracking the volume of spam in relation to United States regulation of CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) can attest to the effectiveness of legislation thus far: Zero. Zilch. Nada.

By now, anyone who was hoping that legislation would have any effect on spam has realized that spammers have taken no notice of the change in the law, primarily because most of them already used methods that make it difficult to trace any spam to them.

Spammers have been apprehended and charged with spamming under state or federal laws. Many others have been arrested and charged with crimes, or sued by

ISPs in civil court. But it's too soon to tell whether there will be enough successful prosecutions to even make a dent in spam.

## **Pattern and Bayesian Filters**

Around mid 2002 there was a buzz in the anti spam community about a paper published by Paul Graham which advocated a technique called Bayesian Analysis as a new means to identify spam.

The technique devised by Paul Graham made use of Bayesian theorem to record the frequency of words used in legitimate email and of those used in spam email. Based on a record of past words used in both categories of email, it is possible to filter spam as they tend to make use of the same words over and over. Today, it is very difficult to find an anti-spam product that does not make use of Bayesian filtering.

Pattern and Bayesian filters are fairly effective, but false positives will block legitimate email. Often block innocent messages about spam. They are sometimes put in place without the recipient's knowledge, aggravated by the fact that normally the filters don't bounce messages to tell the senders they were blocked.

[EmailXT uses a receipt mechanism that helps the sender know if the sent message has reached its destination. Also, standardized error messages help pinpoint the nature of a failure.](#)

At present spammers attempt to disrupt Bayesian filters by including random text or even long passages of literature in their spam email messages. This trick of adding this 'innocent' text to spam emails helps tip the balance and allow the message to be weighed as legitimate.

After becoming apparent that spammers were subverting Bayesian filters, a conference at MIT in January 2005 tried to escalate the spam wars by finding ways to close the loopholes in Bayesian filters. The conference drew some of the brightest minds working on the spam problem, but it was evident that technical solutions were failing. Solutions presented at the conference were no more than Band-Aids patching the holes in the filters discovered by spammers.

## **Whitelist filters**

Whitelist filters are mailer programs that learn all contacts of a user and let mail from those contacts through directly. Mail from strangers is redirected to other folders or challenged. If users respond to challenge, their mail is delivered and they are whitelisted.

There are simple responses (just reply) and fancy ones (Identify the object in this

picture) which can't be automated. Today just replying works but it won't work forever.

On the positive side, whitelisting is extremely effective with no false positives and can be used in combination with other tools (filters, stamps etc.).

On the negative side, it makes anonymous email difficult and delays email from new contacts. It could also turn into an arms race with spammers if they decide to try to automate response to challenges. Mailing lists must be individually whitelisted.

EmailXT relies heavily on the whitelist approach to keep spammers out of your mailbox. This approach adds new hurdles for anyone who wants to communicate with you, like spammers. But also innocents. This is a price that we all have to pay for privacy. But keep in mind that EmailXT has alternatives for this approach. For instance, you can add passcodes to your mailbox, so that people can bypass the whitelisting procedure. By controlling the distribution of your passcode, you can keep your mailbox away from spammers but giving free access to strangers that obtained your email address through proper means. If one of your passcodes is compromised, you can revoke it and set a new one. You may have multiple passcodes in effect at the same time.

## **Hiding your address**

Many are reacting to spam by refusing to reveal their email addresses in public and sometimes even in private, for fear of a privacy-invading deluge of spam.

Other practices include using temporary addresses for replies that are shut down after a few weeks, addresses written in natural language that computers can't understand, or using a different address every time and closing off addresses being spammed.

Although it cuts back on spam, spammers have other ways to get addresses. It is a cumbersome practice. The worst is that it makes it much harder for legitimate people to contact you.

Even if no one discloses your address, spammers can still get it through dictionary attacks. In a dictionary attack, spammers try sending a test mail to millions of possible addresses. Any that don't bounce are probably valid.

Using EmailXT, you don't have to hide your address. With EmailXT, simply getting your email address is not enough to communicate with you. Your new contact must either have a valid passcode or go through a simple, yet unavoidable relationship approval process. If, for any reason, your passcode is no longer effective, you can switch to a new one.

## Challenge-Response

When you get an email from someone you haven't had mail from before, a challenge-response system sends back an email to that person, telling he must go to a web page and fill out a form before his email can be delivered.

The advantage of challenge-response systems is that they let through very little or no spam at all. The disadvantage is that some consider them rude.

The other disadvantage of current challenge-response filters is that much legitimate mail will either be lost, or delayed until it's too late to be useful. Suppose a friend of yours is going to a party tonight and decides to invite you. Your system replies with a challenge. But he doesn't see this until he checks his mail again the next morning, which by then is too late.

There are also some technical objections to current challenge-response filters. For instance, what happens when spammers decide to use some innocent person's address as the from-address in a spam campaign? What happens when spamware authors figure out how to spoof challenges? How can blind people pass those challenges?

EmailXT features some measures to fix most of the current challenge-response limitations. For instance, challenges will only be sent to people who had initiated a relationship. Also, challenges can be customized, rendering any specially crafted algorithm useless. Challenges can also be sent as text messages, so that visually-impaired people can go through the process without trouble.

It has been claimed that the effectiveness of challenge-response decreases when people receive 200 emails a day from new sources and "asking them to respond to 200 mails a day just to authenticate is unacceptable".

However, it is the sender – not the receiver - that undertakes the authentication, so it really doesn't matter how many new emails arrive from unknown senders because it's the senders who must respond to the challenge.

It is possible that some legitimate users may send 200 emails a day to new recipients. If all those receivers had a challenge-response in place, then the sender would have to reply to 200 challenges. But who would send out that many emails to new recipients every day? Newsletters? A sales or marketing company? Such companies would probably not object to the effort involved in solving 200 challenges. As legitimate senders they would most likely thank the opportunity to have their email not classified as spam and discarded.

Filter-based and community-based products just escalate the problem, as spammers continue working to find new ways around them. But the permission-based process (including challenge/response) blocks 100% of unsolicited spam without the need for continued monitoring, attempts to measure trust, or other heuristic methods.

The main objections to permission-based systems stem from misunderstandings or from poor implementation by some software vendors, and protests from a few people who feel they have the absolute right to throw their email at anyone they choose. That might have been acceptable in the beginning, but it is no longer realistic in our current situation.

EmailXT does not use a pure Challenge-Response (C-R) system, but a Request-Challenge-Response variation: It is the sender that initiates the challenge procedure and not the recipient.

Also, request, challenge, and response messages are all categorized: These messages have their own type in the EmailXT universe and can be uniquely identified and processed.

EmailXT avoids the commonly claimed C-R pitfalls: No nasty message loops will occur when two correspondents have a C-R system in place; Challenge spoofing will not be possible because the sender must initiate the challenge process himself. Stray challenges will just be ignored.

## **Community-based**

In a community-based spam filtering system, you start with a neutral trust rating. Each time your classification choices match those of the community, your trust rating increases; when you unblock a message that others call spam, your rating decreases.

Once a few trusted subscribers identify a given message as spam, the central database records a digest of that message and blocks it for all other subscribers.

This is currently one of the most effective ways to fight spam today. But it has its problems: Since a central database must be accessed by subscribers on the Internet, it may be subject to a DDOS attack, rendering the system unusable for hours or days. It is a third-party system, therefore you must subscribe and pay for it. You don't have it under your control. And most importantly, this system relies on a delay between the time subscribers get the messages and the time a classification threshold is reached to make it effective globally. This means you cannot use this system if you want to quickly get your incoming messages. If you check your email too fast, you will receive a larger quantity of spam messages.

EmailXT is a decentralized system. Each peer (you) is a self-contained system. There is no need to subscribe and pay for external services, or rely on the continuity and availability of external businesses.

# Impact of current anti-spam measures

## False positives

False positives are legitimate emails that get mistakenly identified as spam. For most users, missing legitimate email is much worse than receiving spam, so a filter that yields false positives is like an easy cure that carries a death risk to the patient.

The more spam a user gets, the less likely he will notice one legitimate message sitting in his spam folder. And the better your spam filters get, the more dangerous false positives become, because when users believe filters are really good, they will be more likely to forget everything being caught.

The most dangerous situation is when a spam-blocker stops a piece of legitimate mail from reaching its target, by simply dropping the mail on the floor with no diagnostic to the interested parties.

If we have false positives, we abandon one of the most fundamental features we want from a mail system -- reliable delivery.

EmailXT removes the need to use spam filters, and consequently the danger of having "false positives" trashed. On the other hand, every message you sent will generate a return receipt on the receiving party, assuring complete reliability to your communications.

A tight filter can give users the feeling they are missing something. But loosening the filters won't assure that all legitimate email will be read either. Workers eager to clean their inboxes often kill messages that look like spam but aren't.

**FACT:** According to Ferris Research, false positives cost businesses about \$3.5 billion a year.

JupiterResearch estimated that in commercial mailings, 12% of marketing email was blocked because of false positives in 2005, down from 18% in 2004. This was an improvement, but still far from marketer's wishes.

## Important messages being blocked

The scariest aspect of the spam battlefield are vaporized messages. Those that simply vanish somewhere in between sender and receiver. What if one of those messages is an important warning, a due notice, a message from a long lost relative, or the deal of your life?

**FACT:** In a recent UK survey, 66 percent of respondents said that legitimate emails they should have received have been blocked by a spam filter. Two thirds of those respondents said this happened on a monthly basis but a quarter of those surveyed said that they experience this problem on a weekly basis. While 51% of those respondents said time wasted was the most significant repercussion, 42% have missed a deadline as a result.

#### Case 1 :

In April 2005, many ISP's anti-spam software backfired in the hurricane-hit state of Florida, where emergency managers in Indian River County discovered that their email weather alerts were being marked as spam.

After an unusually busy hurricane season, around 4,200 people signed up for the county's email alert service that offered quick alerts on hurricanes, tornadoes and other weather emergencies.

But not everyone received the alerts, as ISP's filters were discarding the emergency emails as spam.

County computer software engineers explained, "Because we send out mail in large numbers, it becomes a pattern for spam senders."

For all who rely on such vital information, it's not comforting to know that while our dependence on email grows, more important messages will get lost in the electronic shuffle.

#### Case 2:

Lawyers at one time noticed they weren't receiving valid emails about lawsuits related to arthritis drug Vioxx, which was pulled off the market by manufacturer Merck & Co. Inc. in 2004. To reduce the number of pornography-related messages, the filter used by the lawyer's agency deleted emails that included "xx", that happens to be the last two letters of Vioxx.

#### Case 3:

The first live run of the Indian Ocean Tsunami warning system turned out to be a bit of a disaster.

It was not a natural disaster of course, but it provided an unexpected result for some users of Apache's SpamAssassin.

Subscribers to the automated email warning system, which sent out an alert for an earthquake off Northern Sumatra that rated 6.7 on the Richter scale, found the Tsunami warning notification deferred as spam.

The problem arises if the open source filter is installed straight out of the box; the messages (usually written in upper case) are not considered spam.

But for anyone who locks down the spam filter, SpamAssassin categorizes the email as spam due to a combination of upper case text in a clear-cut format forwarded by a hidden sender.

With the spam filters locked down, the warning message - written in the original in upper case letters, of: "THERE IS A VERY SMALL POSSIBILITY OF A DESTRUCTIVE LOCAL TSUNAMI IN THE INDIAN OCEAN", rates a spam score of 3.7 out of 10.

Reliability is a key aspect of EmailXT: The sender always knows what happened to their messages. A return receipt is always returned when a message reaches the recipient's inbox (not the mailbox). And if an error occurs, a specific error code will help you understand what happened and act accordingly.

## **Mailing list messages being blocked**

**FACT:** Top ISPs and web-based email providers did not deliver 21 percent of permission-based emails to consumers' inboxes during the first half of 2005, according to an email deliverability study. In 2004, 22 percent of permission-based email was not delivered to their intended recipients. Over 1/3 of consumers say spam filters are blocking emails they opted to receive from trusted sources.

It is suspected that legitimate mailing lists that may target subjects that overlap with today's spam subjects may be in deeper trouble.

Newsletter features that may undermine its deliverability are:

- Use of words like "free", "buy" or "remove me"
- Too much HTML, graphics or text
- Unusual font colors and table layouts
- Subject lines containing "ADV"
- UPPER or lower case letters in body copy

Since you establish a relationship with a mailing list server, you don't need to worry about deliverability issues since EmailXT automatically accepts email from trusted sources. And when you no longer wish to receive a newsletter, you have a simple and universal unsubscribe method: just revoke the relationship and the sender is automatically notified. There is no need to follow complicated, case-by-case unsubscribe procedures.

## **Company products that seem like spam**

Another good example of this is what happens when you refinance your home loan. You may think your bank is being really unresponsive, and they will probably think the same of you. It turns out that your own spam filters are picking up on the words “refinance” and “interest rate” and saving you from what the filter thought it would be blatant spam.

The unfortunate truth is that spammers and phishers are doing business in areas that also are home to legitimate businesses, such as real estate, finance, banking, medicine and software sales.

If your company’s legitimate business overlaps with the spammers’ business and you use email for anything marketing-related, you surely will have a problem. Even if you send your emails only to people who have actually opted in, there’s a really good chance that the spam filters at the recipient end are dumping your email. There’s also a good chance that your own filters will discard incoming email referring to your own product, unless your filter has the capability to be taught the difference between spam email and email-like-spam.

Marketers don't need to worry to send their advertisements through EmailXT. First, they can only send to people that really had "opted-in" by previously establishing a relationship with the marketer. Second, people need no content filters so marketers can freely use words like "mortgage", "pills", "share stock", even "penis" and "Viagra"!

## **Other anti-spam proposals**

Technical solutions actually abound, but they cost money, time or both - a prospect that frustrates overworked business owners who need to focus on growing their companies.

### **E-stamps**

The concept behind e-stamps is good -- if there can be a small sending cost associated with sending an email, the problem of spam will go away. At least the random spam by those that are filling our mailboxes. Serious marketers might still continue since they are willing to spend 50 cents to a dollar to send direct mail pieces to large entities.

### **The reasons why e-stamps won't work**

First, there's no digital infrastructure for small transactions. Past attempts to build a micro-payment system have failed or faded away. There are payment systems like

PayPal, but their costs make it impractical. Payments like 25 cents are out of the question.

Many systems have a chicken-and-egg problem, and only some overcome it. At the start, few people would be offering such stamps. That means you really can't reject all mail that doesn't come with them. In fact, you can't even do anything special to it. Only when a good fraction of your incoming mail has stamps will you be able to use the presence of such stamp to make a filtering decision.

But until people are doing that, what's the point of including the stamps?

EmailXT does not suffer from the chicken-and-egg problem. Two users are enough to start an effective EmailXT network. This network will grow as more people join in and relate with the existing users. Isolated EmailXT networks may connect at any time, increasing its reach. And you can use both email systems on the same address simultaneously.

Virus vulnerability : If e-stamps are done with money instead of CPU coin, there becomes a giant incentive to write an email virus that causes millions of people to email a dummy offshore email address, where you take the money and run.

Mailbox Ownership : If your ISP owns your inbox, then they can set any rate they want for mail delivery. They can even cut a deal with advertisers for low-cost delivery of advertising to your mailbox. The recent AOL/Goodmail case is a living example of this. With e-stamps, there is a big incentive for your ISP to own your inbox.

Tax Issues : When money starts flowing around as it would with money stamps, taxes always become an issue. When stamps are redeemed they create income. Income is subject to taxation. In other parts of the world, value-added taxes might be VAT paid by the message creator. Messages flow accross the world. Do you feel a nightmare somewhere?

Liability : Who would be liable for the accuracy of validation and redemption information from e-stamps? With no legal liability, nothing would stop a spammer from setting up his own stamp-issuing operation, and then giving free e-stamps to all his friends.

## **CPU payment systems**

An idea not involving money was developed: Some people have suggested the idea of "CPU stamps".

One of these systems is called HashCash:

The theory behind HashCash is that a sender of a legitimate email message attaches a header line which proves that he has invested a certain amount of computer time into solving a small puzzle. The receiver can, at a much smaller computational cost,

verify that the sender had indeed solved the puzzle. This can be compared to a kind of numerical stamp, where the 'cash' part is the computational power invested by the sender.

It is expected that spammers, whose business model relies on the ability to send large numbers of messages with very little or no cost per message, cannot afford such an investment into each individual piece of spam. Receivers could verify whether a sender made such an investment and act accordingly.

One critical problem with HashCash is that it is not clear whether the current specification is good enough, allowing good people to get on with their work while preventing bad people from getting on with theirs. Botnets or cluster farms may allow spammers to increase their processing power enormously, effectively reducing the burden of validating individual messages.

Also, according to Moore's law, computers continue to get faster. So the difficulty of the calculations required must be continuously increased over time and we may run out of bits too soon.

EmailXT is computer-power independent. It relies on human capabilities to validate new relationships, so CPU speed evolution is not an issue. On the other hand, as computers get more powerful, they could be used to simulate human capabilities. To counteract, EmailXT does not rely on a static validation method. The current challenge-response system employed by EmailXT can evolve and replace current methods by other cryptographic token systems or biometric verification.

## **Sender authentication schemes**

Currently, several groups are pushing their own sender authentication protocols. Apart from any technical aspects, each of these groups have their own conflicting agendas and as such the evolution of sender authentication schemes have had some bumps in the road.

SenderID is a method for a domain to specify which hosts are allowed to send email on behalf of that domain.

SPF (Sender Policy Framework) is a method for a domain to specify which hosts are allowed to send email on behalf of that domain.

DKIM is based on cryptographic signing of entire messages or message components.

Evidence is building up to suggest that spammers are the most enthusiastic adopters of SPF and the other email authentication methods, to fool users and anti-spam filters into believing their messages are legitimate. Technology designed to prevent phishing and other nasties is being turned against the very people it was designed to protect.

**FACT:** MX Logic tracked a sampling of 17.7 million messages that passed through its servers June 2005, and found that of the 9% from domains with published SPF records, 84% was spam! Of the even smaller number of messages from domains with published Sender ID records (just 0.14%), 83% were spam.

The effectiveness of these protocols is further compromised by the fact that many legitimate senders have yet to adopt either SenderID, SPF or DKIM.

Sender authentication schemes can have limited effectiveness against phishing, but have no effect whatsoever on spam. The proof is that most of their early adopters are... spammers themselves!

EmailXT authenticates senders by enforcing a relationship-establishing procedure on an individual basis. Attackers may still send messages with forged headers, but missing relationship codes and encryption keys will render those attempts useless.

## **Centralized reputation/authentication systems**

Recent speeches on the subject of stopping spam have been moving closer to reliance on centralized systems to authenticate the senders of email. Any such system would be problematic in the extreme for the following reasons:

**Subversion of Freedom :** Central email identity or authentication systems are actively destructive to a free society. Identity systems have a chilling effect on free speech from both the speaker's and the listener's perspective.

**Technical Failures :** Managing identity systems is hard work. It is a very expensive and time-consuming process that makes most system administrators cringe. The more identities you need to manage, the more expensive the system becomes. Centralized identity systems would put unnecessary friction into the Internet's operation.

EmailXT does not rely on a central authority or database. Therefore it is immune to DDOS attacks or hijacking. In addition, your personal and critical data are stored locally, so you can set your own security policies. In case of emergency, you can always pull the plug!

**Trustworthiness:** Just as money stamps have problems with forgery through spammer ownership of a stamp issuer, authentication systems are prey to a similar vulnerability. Nothing would stop spammers from setting up multiple identity-issuing organizations and co-mingling their spammer identities with those of legitimate users. Similarly, a spammer-owned identity shop could simply validate any identity presented for verification, allowing them to continue to spam.

**Identity Control :** Databases as large as one for worldwide email identities would have unavoidable data trustworthiness problems. The much smaller TSA database

cannot accurately keep track of who can fly and who can't. IRS and Social Security offices also have similar problems.

Another issue of identity control is deciding under what conditions an identity can be revoked - to shut off a spammer, for instance. Whatever process is chosen, it will be subverted to shut off identities for reasons other than spam. For example, would activists criticizing the war in Iraq still have email access if the government could target them for shutdown?

All of these issues make identity be systems too dangerous for a free society to contemplate. Any decentralized system that meets end-user requirements will work far more reliably than any centralized infrastructure system.

## **Spam and email management in the enterprise**

Findings from a report produced by a global research firm that recently conducted in-depth interviews with employees at 82 Fortune 500 companies, identified two important results:

**FACT:** Spam is still on the rise. The average employee received nearly 7,500 spam messages in 2004, up from 3,500 in 2003.

**FACT:** Employee productivity continues to be hurt. Average lost productivity per employee was 3.1% in 2004, up from 1.4% in 2003.

Companies are faced with the ever-increasing challenge of not only dealing with the inherent problems caused by spam, but also protecting themselves from on-going attacks.

## **Checking the quarantine folder**

Putting spam email in a quarantine folder, where users can later inspect at their leisure and retrieve any good mail that accidentally wound up there, sounds good in theory.

But spam quarantine hygiene isn't fun. It's boring, and it actually exposes you to the very spam you were trying to get away from in the first place. And if you don't occasionally take a look, you might miss an important email that was mis-classified or end up with a stack of spam to go through when you do need to retrieve something.

You don't need quarantine folders with EmailXT, and therefore you don't need to spend time swifiting through it to see if a legitimate message got dumped.

## **Managing a whitelist**

The problem in a whitelist is that it is one more thing that each and every user needs to maintain, or else there is a risk of missing emails.

You'll never miss mail from anyone on your whitelist, but it might delete mail from some people you have given your business card to.

The EmailXT address book inherently uses a whitelist approach. However, whitelisting contacts are automatically maintained by the system. And if you want to give your prospects a direct way into your mailbox, just include a valid passcode in your business cards. Those receiving them will be able to send you direct messages by using that passcode. If they omit it, they will go through the relationship approval process and the message will still be delivered.

## **Important messages lost or delayed**

No matter how you manage it, after you have a spam filter in place, a computer starts making decisions about what email you get to see and what you don't. You have also introduced a new point of failure into the mail delivery system, which could behave in all sorts of annoying and unhelpful ways.

Truly lost mail, with no clues to what might have happened or where it might have gone, is not common, but can happen. Now that more than just a couple of servers are talking to each other and delivering the mail, the chances for lost mail have increased.

When email isn't working correctly, it's already hard enough to diagnose the problem. Now imagine adding new places where it may fail into the picture. That's just what you are doing when you add a new spam filter.

EmailXT communication is reliable since return receipts will inform senders of the delivery status. You still may not know that an important message addressed to you has been discarded. However, the sender will know, and can do something about it to make it through to you.

## **The filter vendor exited the market**

The market for spam-killing technology is still new, and it's quite common for vendors and manufacturers to fail or to be purchased by other players in the market.

EmailXT is an open standard. You don't need to rely on a single private entity. Standards survive any company mergers, downsizing, bankruptcy, sell-outs or policy changes.

## **Filters that are no longer effective**

Spammers are constantly trying to figure out how to get past spam filters. In most cases, they also own the same spam filter you have, and they test each of the items they want to send you through that filter before starting a campaign. Therefore, over time, any filtering technology will become less effective in blocking the new spam techniques.

A filtering vendor must constantly adapt its technology to meet new challenges from spammers. For many companies and individuals, that means a subscription-based approach, translating into added costs. For others, this adaptation may take the form of software updates, which refresh the software package several times each year. In some cases, your vendor's approach is a dead end, and there is no way for it to update other than starting from scratch with a new system.

Constantly updating filters is an unreliable, costly and time-consuming method. EmailXT needs no upgrades because it doesn't rely on filtering methods. When your correspondents answer a challenge generated by your EmailXT mail client, they are filtering themselves. And if you think InfinityXT's challenges are getting too easy, you may come up with your own, custom-made challenges.

## Chapter 3: Threats by Email

### Phishing

Phishing attacks use both social engineering and technical disguise to steal consumers' personal identity data and financial account credentials. Social engineering schemes use 'spoofed' emails to take consumers to counterfeit websites designed to trick recipients into giving financial data such as credit card numbers, user names, passwords and social security numbers. Spoofing brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond.

Most methods of phishing use some form of technical deception designed to make a link in an email appear to belong to the spoofed organization. Misspelled URLs or the use of sub-domains are common tricks used by phishers.

The biggest challenge the industry faces now is the loss of consumers' trust. The continuing growth in phishing attacks and its big media coverage have caused consumers to look at all commercial email messages with fear, uncertainty and doubt. Phishing has had a bigger damaging impact on the email medium than spam. While spam can be potentially harmful, it is for the most part just an annoyance. However, if a consumer is caught in a phishing net, the results are much more damaging and can cause serious financial loss.

EmailXT can stop phishing very easily: When establishing a relationship, several system-level messages are sent between the requesting party (sender) and the granting party (receiver). If a scammer is using a forged address, he simply cannot get your challenge message that he needs to answer and validate himself. The message would simply go to the forged address, and then rejected since the forgery victim didn't start a relationship with you. In addition, a certificate from a root CA can increase security even more.

Here are examples with increasing levels of sophistication:

- CitizenBank is the forgery victim.

#### Scenario A:

- Scammer sends a relationship request, pretending to be from [accounting@citizenbank.com](mailto:accounting@citizenbank.com).
- Your email client replies with a relationship challenge, sent to [accounting@citizenbank.com](mailto:accounting@citizenbank.com).
- CitizenBank didn't request a relationship with you, so your challenge is ignored.
- No relationship is established.

## Scenario B:

- Scammer gets hold of one of your passcodes.
- Scammer sends a message to you pretending to be from `accounting@citizenbank.com`.
- Your email client sends the relationship acceptance message to `accounting@citizenbank.com`.
- CitizenBank didn't request a relationship with you, so your challenge is ignored.
- No relationship is established.

## Scenario C:

- Scammer innocently relates with you to get your public encryption key.
- Scammer assumes you are a CitizenBank customer and tries to send a message directly to you
- Scammer uses your public key to encrypt a message to you, pretending to be from `accounting@citizenbank.com`.
- Your email client decrypts the message but finds no valid relationship keys (the genuine keys are stored only on your computer and bank's computer).
- Your email client discards message and warns you.

So, even if the scammer had the chance to get your banking info, he probably wouldn't do it in the first place. And that's because it would not compensate to do phishing on a case-by-case method.

## Viruses and worms

A computer virus is a computer program written by someone with malicious intent. It usually has two objectives:

- To reproduce itself so that it may spread
- To do some sort of job, which may vary from displaying a simple message on startup to causing serious damage to your files and your operating system. This job may not be done as soon as you acquire the virus; many viruses are written to be activated on particular dates, so that they have time to spread before they are detected.

Back in 1993, there were 3200 known viruses in the world. Today, there are more than 42,000, although only 200 to 300 of them are actively spreading. Around 10 new viruses are released each day, and each generation gets smarter than the last.

There are several kinds of virus: nowadays, the great majority are spread by email, but some are delivered through executable programs or MS Office documents, and some will also infect your computer if you boot it up with an infected floppy disk or CD.

Viruses used to take months or even years to spread, but current strains can get around the globe in minutes using email. In addition, the market supremacy of Microsoft Windows and Outlook makes it easy for viruses to infect millions of computers in a short period.

Currently it takes anti-virus software vendors between 1 and 4 hours to detect and analyze a virus, produce an antidote, and distribute it among suppliers. But it took just a few seconds for a virus like LoveLetter to span the globe!

Today's viruses and worms typically spread by email. They will scan your computer for email addresses of your friends and co-workers and send a copy of themselves in a disguised message pretending to be from you. However, sending a message by just having an email address is not enough with EmailXT. Access to the protected address book is necessary to obtain additional relationship information that must be sent along with the message for it to be accepted on the other end.

## **Spyware**

You have heard everywhere about how important it is to have a firewall on your network, usually by installing a broadband router. Router firewalls keep crooks on the Internet from directly reaching the computers in your home. There is however a different kind of threat on the Internet - a more subtle, deceivable, and sometimes nearly undetectable threat - Spyware.

Spyware can be any program that secretly tracks or records information about you, your personal information, Internet habits or computer use. Usually these programs have the ability to report back to a central database on the Internet without you ever knowing about it. Since many people now have "always-on" broadband Internet connections, it is easy for spyware software to report it's findings whenever the creator feels necessary.

Spyware can be delivered and installed on your computer in many forms. It is sometimes included in the install package of many popular shareware programs. Sometimes it comes installed in your favorite operating system or even directly from the manufacturer!

Today, the most frequent method of spyware dissemination is through specially crafted web sites, bulk emailing or virus outbreaks.

## **Business Disruption**

An increasing number of corporate data breaches, combined with a continuous rise in the sophistication of spyware threats and distribution methods, made 2005 the biggest year for spyware so far, according to a report issued by Webroot Software, an anti-spyware vendor.

In 2005, half of US businesses reported a spyware-disruption that resulted in lost revenue, a statistic that was confirmed by a recent FBI study which concludes that computer-related crimes such as spyware cost \$62 billion to U.S. businesses. It is 10% more than identity fraud and 60 times more than the cost of telecommunications fraud.

EmailXT cannot do much to combat spyware outside the email ring. However it may help it by stopping this kind of threat to be sent by email.

## **Zombie networks**

Zombies have been used extensively to send spam. Between 50% and 80% of all spam worldwide is now sent by zombie computers. This allows spammers to avoid being detected and reduces their bandwidth costs, since the unsuspecting zombie owners pay for their own bandwidth.

Over the past year, security experts have become increasingly worried about botnets, also known as zombie networks. Once used mainly by hackers for rivalry battles, these large networks of compromised computers are now being used as a tool for groups of criminals determined to make money through identity fraud, spyware installation or sending massive amounts of spam. Anyone whose computer gets infected with bot software risks having sensitive information such as credit card numbers and bank account passwords sent to the criminals.

According to a HoneyNet Project report, some of these networks are made up of more than 50,000 computers. The origin of the zombie machines may change on a daily basis as machines can be infected anywhere in the world, with the largest percent of zombie originations between China and the United States.

Unfortunately, if your computer has become a "zombified" machine, EmailXT cannot do anything about it. However, it does a lot indirectly, since it protects all EmailXT users from being spammed from your computer, and ultimately renders the spam-zombie-army model unfeasible.

# Chapter 4: Security, Accountability and Reliability

## Security measures

**FACT:** Research demonstrates that 1 out of every 500 email messages contains confidential information, yet less than 1 percent of non-spam corporate and government agency messages are encrypted (Source: Gartner, October 2004).

Recent high-profile data security breaches have resulted in 5.8 million consumers being exposed to identity theft.

Companies lose hundreds of millions of dollars every year in pirated intellectual property, including leaked source code and design documents. The average cost per incident is \$2 million, according to the Aberdeen Group.

The vast popularity of email has created a requirement to send mail securely over the Internet. Email that is sent unencrypted could be intercepted by casual or targeted efforts. Therefore, most organizations have a prohibition against sending classified information over the Internet, which has resulted in

- users ignoring such policy, thereby creating a security risk
- users resort to more costly (like overnight delivery) services or less efficient communication methods like the phone or face-to-face meetings.

EmailXT's built-in security allows your company to safely send any kind of sensitive data. Using EmailXT in your organization will:

- Enforce a reliable security policy
- Ensure data privacy in-transit
- Adds trust to your corporate and B2B actions, agreements and transactions

Any issues involved when business, contractual or legal aspects apply, are more complex and less well served by today's email. Authentication improvements, like being confident about the individuals and servers that you are communicating with, are central to the broader future use of email. However, the basic email protocols, especially SMTP, are not intrinsically secure, and making improvements to the Internet's infrastructure is very difficult.

When a mail server sends you an SMTP message, the only thing you know for certain is the IP number of the sending server. All other parts of the message and transaction can be spoofed.

Just because the current messaging infrastructure is insecure doesn't mean that messaging itself has to be insecure. With EmailXT, spoofing is not possible since secret relationship codes have to be sent along with the message to authenticate it. An attacker may fake a message from a trusted source using your public encryption key and send it to you. However, due to a lack of authentication, the message will be discarded.

## Reliability

Sometimes the only way to know whether an email got through is to make a phone call.

**FACT:** According to Microsoft studies, one in 140 e-mail messages disappears without a trace. On a recent Reflexion survey, 99% of respondents reported missing legitimate email to spam filters. Of these, nearly half lost between 10 and 50 messages!

As spammers identify new ways for sneaking their junk past spam filters, service providers' technical efforts could put even more legitimate mail at risk.

Spam and spam-fighting have in some cases eroded the reliability of the mail system. A lot of email now gets filtered out. A typical user might lose anywhere from a legitimate message every few months to as many as five in a single week, tells Ferris Research.

A lot of spam-classified email simply ends up in junk folders that many recipients never check. But sometimes ISPs reject such messages at reception time, meaning recipients have no control even if they turn their spam filters off. In these cases, senders won't get non-delivery error messages, even though Internet standards encourage them.

EmailXT features a return receipt policy. Each message sent requires a return receipt. This way you always know if your message has really been received at the other end. If you receive no receipt in a predefined amount of time, your email user agent may warn you and then send the message again.

Privacy advocates will complain that this is a privacy breach since the sender will know the recipient's reading habits. However, these EmailXT receipts, unlike the current email system's receipts, are not generated when the recipient reads the message. They are generated when the recipient's mail user agent receives the message into its inbox. In addition, a return receipt mechanism is absolutely necessary to have a reliable email system.

## Archiving & Accountability

Whether it involves private customer or employee data, financial records or proprietary product data, the security of confidential information is increasingly being subject to both corporate policies and government regulations.

HIPAA, Sarbanes-Oxley, California SB 1386 or Gramm-Leach-Bliley are just a few of the laws that require strict accountability of all confidential data.

For example, HIPAA requires that all messages which contain protected health information must be encrypted. Also, the Visa-MasterCard Payment Card Industry Data Security Standard requires companies to encrypt the transmission of transaction and customer information.

It is also becoming increasingly necessary to retain and manage email archives. This is frequently driven by the need to comply with regulations, such as HIPAA, Sarbanes-Oxley, SEC 17a-3/4, and NASD 3010. An important driver is also the value of accessing past email and mine the knowledge it contains.

Email retention and archiving solutions capture and store email messages in dedicated repositories. They let users find and retrieve messages. They also manage archived emails over their entire life cycle.

**TREND:** The email archiving market is expected to grow from \$800 million in 2006 to nearly \$7.8 billion in 2010.

**TREND:** A new study by the Radicati Group expects European revenues for the compliance and email archiving market to grow an average of 74% per year from 2005 to 2009. That's an increase from €207M in 2005, to €1.8B in 2009.

The Email Archiving market in Europe is increasingly being driven by compliance, which is gradually overtaking concerns about storage. While in 2004 storage was the leading driver, regulatory and internal compliance have been the key drivers in 2005.

EmailXT will help you comply with current accountability and archiving regulations. For instance, the secure nature of EmailXT's communication will help you comply with HIPAA's privacy requirements.

A planned InfinityXT enterprise version will enable you to archive your emails in a central repository for later archiving and retrieval.

## Chapter 5: About EmailXT

EmailXT is an evolution of the current email protocol. It extends email beyond its current capabilities but without changing its infrastructure.

Most analysts say that it is almost impossible to replace the SMTP protocol at this point due to the sheer penetration of the Internet and the huge number of email servers in existence. EmailXT avoids this dead end by relying on the existing SMTP/POP protocols. Security is then built at a higher level, meaning that any spoofing attempt at the SMTP level will be detected at a later stage.

EmailXT is like a new email network inside the existing one. The emphasis is put at the MUA (Mail User Agent) level. Email transport can be dumb as long as the clients are smart.

To an email server, EmailXT messages are just like any other present-day message. However, encapsulated in the regular email format, lies a completely different world. Messages are no longer sent in the clear, and authentication plus any useful data is crunched and encrypted in a solid block of data.

Since compliant applications only accept EmailXT messages, anyone wanting to send you a message must play by the EmailXT rules. You are effectively shielded from the jungle that is today's email.

EmailXT is a completely decentralized system. It does not rely on a central server or service. Each Mail User Agent is an autonomous unit.

### Deployment

One of the greatest strengths of EmailXT compared to other past proposals is its ease of deployment:

To make the switch from the existing email system to EmailXT, you just need to install a compatible application like Infinity XT, answer a few simple setup questions, and you are ready to go.

InfinityXT works the way you expect in an email client. In a few hours you can learn and master its capabilities, and in a short period you won't even notice that you are using a completely different email system.

There is no need to setup server accounts, or pay monthly fees to any service.

EmailXT works with your existing email address. While you are transitioning from the old to the new email system, you can still check your old-system emails in your new

EmailXT mailbox (as long as you check EmailXT mail first). This guarantees a smooth transition.

As time goes by, you will connect to more and more friends and business partners using EmailXT and your mailbox slowly returns to life. You will rely less on the existing email protocols, and rely more on EmailXT. After a while, you will be ready to dump your existing email client.

## **Relationships**

With EmailXT, your mailbox is no longer an open, abused mailbox. Machines can no longer send you unsolicited email. Only real people.

There are several levels of control: With regular relationships, anyone wishing to correspond with you must first establish a relationship, going through a simple approval process.

With passcodes, you can give immediate access to your mailbox, avoiding the usual approval process. This way you can be instantly reachable, but with the ability to "pull the plug" if your passcode gets compromised.

Once you establish a relationship, a secure communication channel is established and you can exchange messages with your correspondent with the confidence that emails are immune from viewing or tampering while in transit.

Trust is implicit in an established relationship. However, different trust levels exist. The two correspondents assign a default trust level to each other. Then, according to each correspondent's policy, the trust level can be raised, thus enabling the sharing of more files and personal information.

## **Anti-spam measures**

With EmailXT's relationship control, the deluge of unsolicited messages stops. Period. The only way a spammer can send you a message is by going through a validation process or getting hold of one of your passcodes (if you use any).

In any case, you can just cancel your passcode and use another one, or revoke the relationship, effectively "shutting the door" on the spammer. Your email address on the spammer's list simply becomes useless.

Under EmailXT a simple email address is useless without a means of authentication: A passcode or an established relationship.

## Privacy

All EmailXT messages are sent encrypted, meaning that only you and the recipient can read the message.

EmailXT uses industry tried-and-tested encryption technologies. Messages are encrypted using RSA public-key encryption and Triple-DES symmetric encryption.

When a relationship is established, RSA public keys are exchanged and used for future secure communication.

You can now exchange sensitive data like personal bank, credit card, insurance or health information without the risk of it falling into the wrong hands while in transit or on a mail server.

**NOTE:** Only messages exchanged under an established relationship will benefit from full-strength encryption. Messages exchanged using passcodes use the passcodes themselves as the encryption session key. Although the passcode is not specified in the message, it should be considered an highly insecure message.

## Ease of use

With EmailXT, some things that were once complex, are now automatically handled by the underlying system.

For instance, dealing with encryption certificates is regarded as being complex and time-consuming. Your EmailXT-compatible application takes care of all certificate exchanges. The encryption certificates are then automatically managed by the Address Book.

The only difference you will notice from the current email system is that you will have to answer a challenge before being allowed to send messages to a new email address. However if you have a passcode you don't even need to do that. Just type the passcode next to the destination address and your message can immediately be sent.

## Virus protection

Email-borne viruses work by bulk-emailing themselves to every email address they can find, wreaking havoc on unsuspecting victims.

With EmailXT, you are effectively protected from this kind of pests since unsolicited

bulk email no longer works with EmailXT. And the protected EmailXT address book is no longer accessible from rogue software.

It must be said that an EmailXT application is not immune to viruses. A user with a poor security policy may fall prey to an intelligent virus, trojan horse or spyware. However, since it is a peer-isolated system, a virus outbreak will probably be limited to a few addresses contained in the compromised computer.

Virus writers normally do a mass dissemination of their virus by bulk emailing it to harvested email addresses around the globe. With EmailXT, that scenario is no longer possible. The virus writer is limited to the addresses in his address book! Even if it gets hold of compromised EmailXT address books, the effort needed to obtain them is far bigger than it currently is. In addition, the outbreak would again be limited to the compromised addresses.

## **Extensions**

Since its beginning, email has been a bare-bones messaging system: It started as a simple, plain text message. Later came the file attachment. Evolution stopped ever since. However, the world didn't stop and email is now struggling to keep up.

EmailXT adds functionality to email beyond the simple messaging application. On top of the basic EmailXT protocol, several non-mandatory extension protocols like tasks, calendaring, forms and file sharing push email to the next level, satisfying demands for a more capable system.

## **Tasks**

Tasks can be easily identified in your personal and professional life. Every day, dozens of tasks must be accomplished to get on with our work or life. Most people keep pending tasks on their heads but as the daily rhythm increases, so does the need for a proper task tracking method.

The corporate environment is the most demanding one: Your boss, your co-workers, your customers, your suppliers, all assign tasks to you. Some have deadlines and others don't, but you need a common, reliable way to sending and receiving task notifications.

To support the management of all your tasks, EmailXT has an adequate extension protocol. It allows you and your contacts to receive, assign and share tasks, as long as trust levels permits it.

## **Calendaring**

Having an organized life today means having control on the upcoming events, meetings, birthdays, deadlines, etc. Additionally, in a wired, collaborative world, events need to be distributed and shared.

The Calendaring EmailXT extension protocol allows all types of events to be set, distributed and shared in your organization or across the Internet. Supporter applications will receive the calendar commands and will manage their calendars locally.

## **Forms**

Have you already been asked to go to the web to fill-out an online form? Do you need to manage surveys, sign-ups, requests, or any other form-demanding need?

EmailXT features an extension protocol that supports forms, allowing you to design one and send it to your targets. Then, they can answer you in an ordered, predictable way.

## **File Sharing**

EmailXT File Sharing allows you to share any number of files with your contacts through your mailboxes. Trust levels and access control can limit who can download and upload and you can also create distinct share areas.

## **The Address Book**

The address book is a core element in EmailXT. Similarly to what happens now, you have contact information stored in it.

However, the EmailXT address book is an active element. Not only it stores the current state of all your relationships and encryption keys, it can also update itself.

With EmailXT, you no longer need to keep your contacts updated. You contacts will do that for you.

Rich media items like ID photos, logos and business cards can also be shared. For instance, anyone can print a copy of your business card remotely.

## EmailXT and Patents

Software patents are seen as evil by most of the IT community. It hinders software evolution and competition between vendors. A protocol that is supported by patents is not going to have wide adoption. The recent SenderID case illustrates this view.

Zorean took these views into account and developed a protocol that is not patent-encumbered, or relies on already-expired patents like RSA encryption.

Zorean plans to go through a 12-month consolidation period after the 1.0 release before submitting the EmailXT proposal to IETF evaluation.

## Infinity XT

Infinity XT is the first of a generation of intelligent Mail User Agents (MUAs) that implement the EmailXT protocol.

Infinity XT has also the role of being the "Reference" application for other EmailXT-compliant mail clients. It means that Infinity XT has a correct and up-to-date implementation of the protocol, and all other applications should be tested against it. This will ultimately ensure the quality of all the existing and future EmailXT mail user agents.

**FACT:** A recent study tells that the desktop email client segment will grow at an average annual rate of 16% over the next four years. Growth in this segment will be driven by corporate demand for collaboration and groupware features.

Infinity XT is much more than an email client. It aims to be the ultimate personal and work assistant, featuring fully-integrated systems. Email, calendaring, tasks, notes, logs and much more, all working together.

Also, it is worth mentioning that Infinity XT is free. Optionally, you may purchase a key that unlocks additional features aimed at advanced users.

## Chapter 6: Specific Scenarios

### Finance

As financial services organizations open up their networks to customers and partners, the threat of spam, virus and denial of service attacks must be taken seriously, not only to avoid any disruption to their business, but also to ensure compliance with corporate governance regulations.

Many messaging challenges are shared by financial services organizations across the globe, and it is clear that a comprehensive secure message management solution can help ease the pressure on many organizations' messaging infrastructures.

A survey conducted by MORI on behalf of BT shows that IT directors in the financial services industry are interested in or planning to continue increasing their budgets for secure messaging. Over the next three years, most surveyed companies expect to spend even more money protecting email and other communication channels against harmful attacks.

Other key findings on this survey include:

|     |  |
|-----|--|
| 86% | view viruses as significant issues for their organization  |
| 81% | agree the threat of email anarchy is real for those companies that do not address message management correctly |
| 78% | consider archiving a significant issue today. In the UK, this figure is as high as 90%                         |
| 64% | see viruses increasing in significance over the next three years   |
| 65% | expect a budget increase for compliance over the next three years  |
| 60% | say they want to increase email interaction with clients and 72% say security is the biggest deterrent         |

EmailXT can easily help the finance sector companies by offering an "off-the-shelf" secure messaging system that will help them stay compliant with governmental regulations. A secure email channel will help customers feel safe about their transactions and orders.

## Marketing

No printing, no postage, no mail house charges. That's email.

Traditional direct mail costs between \$1 and \$3 per recipient and can take over a month to complete. With email, the cost can be reduced to pennies per recipient and completed in a couple of hours. The response rate of opt-in email was 50 times greater than banner ads and 5 times greater than direct mail. Instead of waiting weeks for responses and test results, you'll could have them in hours. Also, email campaigns are fully trackable, with up to the minute statistics.

These are the reasons why so many businesses turn to email as their preferred marketing channel.

Email marketing is critical to the success of your business. It doesn't matter if your business is online or not, email marketing will save you money, build customer loyalty, increase brand awareness, drive traffic to your website, create sales, and ultimately increase your profits.

Email is effective, there is no arguing with that. It works amazingly well for marketers who know how to use it. Return on investment for email marketing tops all other channels except for telemarketing.

This past holiday season provided evidence of a clear consumer shift toward online commerce. In its Holiday eSpending Report, eMarketer reported that online shopping during the 2005 holiday season topped \$30 billion, a 30% increase over the same period in 2004.

Despite the assault email marketing is suffering from spam and phishing, and even with the erosion on delivery rates inflicted by individuals and corporate filters, and regardless of the sheer email overload in most people's inboxes, 71% of US online advertisers used email marketing in 2004. In 2005, this figure has raised to 83%.

**TREND:** Email marketing is expected to become a \$9.4 billion business in 2006.

However, email marketers continue to suffer damages caused by spam and phishing. The lack of market friction is one reason spam is such a big problem. Barriers to entry are minimal or non-existent, and the market is flooded with spam as a result. No means exist to distinguish legitimate marketing messages from spam. Legislation has failed to reduce the flood of spam. The CAN-SPAM Act took effect in 2004, but the problem is worse than ever.

Legitimate marketers should be concerned about this trend: the probability of their messages being perceived as spam increases, which would result in messages being blocked by ISPs or deleted by the recipient without being read. Filters used by ISPs frequently reject email from legitimate businesses that is in accordance with CAN-SPAM and other laws. Even when using double opt-in lists, businesses

sometimes find their messages bounced or routed to the spam folder.

Marketers can build their distribution lists on top of EmailXT's mechanisms without the fear of having their messages rejected by the recipients. Every relationship established between a marketer and its prospect is a true opt-in mechanism. This is a win-win situation: Marketers will have a targeted and certified list; Subscribers are safe from fraudulent opt-ins and can revoke at any time.

In addition, EmailXT provides an universal subscribe mechanism: To unsubscribe a newsletter, just revoke the relationship. The marketer will receive a notice message and may act accordingly, removing the user from the list. It is important to say that there is no risk of non-compliance with EmailXT: If the user revokes the relationship, there is simply no way for the marketer to reach him.

Many businesses are seeing a considerable drop in email marketing service revenues. And the problem is that spam continues to flood inboxes, crowding out email messages and newsletters from legitimate email marketing efforts. It's a problem people face in the permission email marketing industry: how can people read their opt-in emails if they have to wade through endless reams of spam?

In an EmailXT mailbox, there is no spam, so your targeted ads/newsletters don't fade out in the noise of spam.

A quote from a past Internet article says:

"Some companies are hoping to make up for it with search engine optimization services, but there's little doubt that everyone in the email marketing industry is awaiting the implementation of a workable anti-spam solution that will overhaul email around the globe and make it impossible for spammers to operate."

EmailXT aims to be that workable anti-spam solution, with some added functionality.

## **Deliverability**

About four of five email marketers surveyed face big challenges getting their emails delivered due to filtering by ISPs and corporate servers, according to a research from EmailLabs, a marketing solutions provider. Around half the 415 marketing professionals who replied to the March 2006 survey told that filtering is their biggest delivery challenge. Bounces and lack of expertise or resources were also pointed as important problems. Curiously, for 90% of respondents, improving the deliverability of email campaigns is not their most important marketing concern for 2006.

| Reported issues with email deliverability |       |
|---|-------|
| Filtering by ISPs                         | 48.3% |
| Filtering by corporations                 | 45.1% |

| Reported issues with email deliverability |       |
|---|-------|
| Hard bounces                              | 31.5% |
| Lack of expertise                         | 25.4% |
| Appearance on blacklists                  | 15.3% |
| Spam complaints                           | 11.8% |

What this means for legitimate email marketers is an increasingly complex set of hurdles that legitimate messages must get through to reach their recipients. The problem of legitimate messages being inappropriately caught in spam filters, usually known as "false positives", is not a small one, as seen from the table above. It is predicted that between 0.5% and 3% of legitimate messages are blocked on a regular basis by overloaded, under-staffed ISPs. It means that with a mailing list of 100,000 users, as many as 3,000 of your customers may not receive the account statement, invoice, offer or newsletter that they requested from you.

**FACT:** Today, online marketers are losing nearly 20% of their reach due to deliverability problems. The average email open rate has dropped from 36% to 27.5% and the average click-through rate also declined from 7.7% to 7.2%.

The war between receivers and spammers made relationships between ISPs and legitimate marketers difficult. A guilty-until-proven-innocent attitude by ISPs is now common. The problem is worsened when ISPs do not provide a transparent mechanism for resolving these deliverability issues.

There should be no deliverability problems with EmailXT messages since every message has to follow strict relationship rules to be accepted by the recipient's mail user agent. ISPs don't need to filter EmailXT messages. Even if regular messages are disguised as EmailXT messages to get through, they will be rejected at the receiver's end, so spoofing attempts will be useless.

Proven marketing techniques have been abandoned so that ISP filters may be bypassed. Messages with images should not be sent because these are suspect. Certain words like "free" must be avoided. Even opt-out instructions may trigger filters. So, instead of composing a message using effective sales techniques, marketers must be more concerned about how their message content will be scored by ISP filters. This reduces the appeal of marketing messages, consequently lowering response rates and related revenue. Also, marketers have had to hire staff specializing in ISP relations for the resolution of deliverability issues.

EmailXT uses a return receipt mechanism that helps the sender know if the message has reached its destination. Also, standardized error messages can easily describe the nature of a delivery failure.

## Health

**FACT:** The American Health Information Management Association (AHIMA) reports that fewer than 40% of health care providers use the convenience of email to communicate with their patients.

The vast majority of health professionals and universities won't correspond with patients because they recognize that there are associated risks:

- Email can be forwarded, printed, and stored in many paper and electronic forms and be received by many intended and unintended recipients without patient knowledge or agreement.
- Email may be sent to the wrong address by any sender or receiver.
- Email is easier to forge than handwritten or signed papers.
- Copies of email may exist even after the sender or the receiver has deleted his/her copy.
- ISPs may have a right to archive and inspect emails sent through their systems.
- Email can be intercepted, altered, forwarded, or used without detection or authorization.
- Email can spread computer viruses.
- Email delivery is not guaranteed.

As most health professionals know, the Health Insurance Portability and Accountability Act (HIPAA) made it really hard to stay out of a courtroom, and brought more and more trouble to keep up with its requirements.

Backing that trend, AHIMA claims that the number of hospitals and health systems who believe they are at least 85% compliant with the privacy and security rules of HIPAA dropped from 91% to 85% in one year.

Personal health status is always sensitive information. Your life may change if details about your health are leaked or intercepted. That's why you talk with your doctor in private. But why do you feel worried about doing it by email? Because you feel email is unsafe? Well, you're right! Today's email is unsafe.

EmailXT keeps your conversations with the doctor private. Just like if you were in his office. You can write a message that will remain encrypted on your computer, be sent encrypted over the Internet, and be delivered to your doctor and still be kept there encrypted. And if, for any reason, a system malfunction occurs and your emails are sent to the wrong place or obtained by an unknown entity, you don't need to worry. Only your doctor has the key to read your messages.

## Children

Spam chooses no ages.

Children, like adults, are bombarded by spam advertising Viagra, drugs, pornographic material and other inappropriate products and services.

| What children are getting on their inboxes |  |
|--|--|
| 80%  | received sweepstakes messages          |
| 62%  | receive information on dating services |
| 47%  | receive links to pornographic sites    |

**FACT:** One in five children opened and read spam, and more than half of them checked their email without parental knowledge.

Parents need to educate their children about the dangers of spam and how they can avoid being exposed to offensive content. However, being continuously alert is almost impossible in today's busy, stressed world.

### TIPS FOR PARENTS:

- Talk to children about inappropriate web content
- Teach children not to give out personal information while surfing
- Try not to be overprotective, and trust your children a little more
- Know your children's on-line friends
- Check email together

Past interviews have shown that around 38% of children did not tell their parents that they had been upset by spam and 22% said that their parents never talked about spam. Nearly one in three did not know whether spam was good or bad for them.

EmailXT helps parents prevent children from being exposed to inappropriate content. With controlled relationships, only approved senders can relate to your children. InfinityXT allows you to be the sole approver of new relationships, so that you can choose who can send email to your children's mailbox.

## E-Commerce

E-commerce is one of the Internet's killer apps. Millions of people buy and sell goods every day through their web browsers.

**TREND:** By 2010, e-commerce on the Internet will be composed of hundreds of

thousands of e-commerce websites, all competing for the attention and wallet of the online consumer. The vast majority of these e-commerce sites will be part-time or home businesses selling a small number of products or services.

Buying always involves payment. And payment always involves giving away personal information. While Internet attacks increase in number and sophistication, consumer confidence decreases.

Unless you are Amazon or one of the big dogs, the perceived trust on your store may not be much. The fear of sending away sensitive information to new, untrusted sources keeps newcomers from really expanding their businesses. The padlock icon on your browser is no longer trustful. Cybercriminals are finding ways to simulate trust, circumvent protections, and faking websites.

So, you receive an email from your favorite retailer, with an irresistible offer. You scramble to the linked page, you sign on, add the product to your shopping cart, enter your credit card details and finally you pressed the Order button... Oh, wait! Did I really bought this on my real retailer's store???

Too late.

You may have fallen prey of a phishing attack. Unfortunately many surfers don't even have a clue.

With EmailXT you can first be sure that the email you received from your retailer is really from your retailer. That way, you may click the email links with much more confidence and security. Just check the email signature to see if it was signed with a key containing a certificate from a certification authority. Confused? Don't worry, the application will do it for you.

## **Web mail**

**FACT:** Today, approximately 67% of worldwide email mailboxes are delivered through a webmail service provider or ISP.

Many users rely today on an online mailbox, accessible from anywhere. The management ease and mobility offered by an online email account continues to attract more and more people.

The downside of this approach is that you completely rely on an external, and sometimes unknown, webmail service provider. You have to trust you provider's security measures. A hacker break-in would immediately expose hundreds, thousands or even millions of mailboxes, depending on the size of the webmail provider. You also have to trust your provider that no messages will ever be lost, corrupted or deleted.

If you have a web-based EmailXT mailbox, you will have to trust your private key and address book to your service provider that, on his turn, has to provide enough security for this sensitive data. So, privacy is not guaranteed and therefore you should not rely on a web-based email account to send or receive important, sensitive messages.

## **Forwarding & Mailing lists**

The most common question asked in recent discussions about recent email authentication proposal was:

"Won't this new [...] protocol break mailing list and forwarders?"

You probably have read all you need to know about email authentication. Still, there are some important details when an email forwarder is involved. Forwarders allow you to have one simple permanent address, even if you change jobs or ISPs. Mailing list servers perform a similar job, forwarding email to many subscribers on behalf of one poster. Forwarders are no problem to an end-to-end authentication proposal like DKIM, as long as the signed message is not modified. Some mailing lists will do this.

The use of a forwarder prevents the recipient from directly seeing the sender's IP address. The incoming IP packets will only have the forwarder's IP Address. You have two choices if you can trust all forwarders. Either you trust the forwarder to authenticate the sender, or you trust the forwarder to record the sender IP address and pass it on, so you can perform authentication on your own.

This gets complicated when there is more than one forwarder. A sender can explicitly authorize a forwarder to send on its behalf. A receiver can trust a forwarder to handle email, therefore designating a new receiver. But there could be some additional MTA relays in the middle. These are sometimes used for traffic aggregation, or administrative and routing control. Just one broken link in the chain-of-trust from sender to receiver, and it is no longer possible to authenticate the sender.

EmailXT does not rely on the IP address of either the sender or the receiver. It just relies on the secret information that is passed between the two related parties. For mailing lists, it's enough for the mailing list owner to keep his EmailXT address book. Whenever a subscriber sends a message to the list server, it just decrypts and echoes the message to all subscribers, just as it has been. It is expected that more processing power is required to encrypt the message to all subscribers. However, the bulk of such encryption is made through fast algorithms so whatever resources you are using today to serve your list, it would be enough for an EmailXT-based mailing list.

Forwarding is not a problem for EmailXT since authentication is done at the entity level. A single entity may have multiple associated email addresses, so any of the listed addresses is accepted as a valid origin.