Why spammers spam
An incursion into the world of spammers

Table of contents

Introduction
How the report was created
Acknowledgements
Starting up
Making Money
Organization
Harvesting
Spam tricks
Legislation
Spammers on spam

Norman is one of the world’s leading companies within the field of data security. With products for virus control, spam control, email control, download control and personal firewall, the company plays an important role in the data industry.
Introduction

Vircom is one of Normans technology partner. It is Vircom that has done this study.

Spammers come from every walk of life, every country worldwide and every socio-economic condition.

A spammers work is one of contradiction; they work in a secretive environment, constantly straddling the fence between legal and illegal, moral and immoral. For this report, Vircom acquired the assistance of three active spammers, all of whom have varying degrees of experience and success as spammers.

Our goal for this paper was not to criticize or judge what these people do or how they conduct their business. Instead, it was to gain a unique window on the world of spamming; to shed the cloak of mystery regarding who spammers really are...

...and Why Spammers Spam.

How the report was created

In order to gain the participant’s full co-operation certain criteria were required:
1) Vircom was not to reveal the real names or the online names of the spammers who participated.
2) Vircom was not to specify the names of the product or services our spammers have marketed.
3) Vircom was not to reveal any personal details regarding the spammers without their agreement.
4) No response was to be altered or changed by Vircom in any way.

How we met the spammers

Because they operate on the fringes of legality, spammers are not easy to contact and communicate with. In general, the spamming community is not a close-knit group. Spammers prefer to work solo or in small groups known as "spam gangs."

For the purpose of this study, Vircom took a direct approach and posted messages on a known spammer’s website requesting for experienced persons to discuss spamming. Following this request, we made contact with several persons, including one of our participants, who introduced us to other members of her spam gang.

At no time did we, at Vircom, disguise our identity. The spammers we spoke with were all aware that Vircom is an anti-spam solution provider.

How we coped with spammer “terminology”

Our spammers refer to their occupation in many different terms: "online marketers, bulk e-mail marketers, e-mail marketers, vertical marketers, crap peddlers, mail bombers, junk e-mailers, porn hawkers" as well as "spammers." To prevent any confusion, we will refer to our participants as "spammers", and to the act sending unsolicited bulk commercial e-mails as "spamming."

Readers experiencing difficulties in understanding spammer terms can refer to another Vircom white paper, “Spam’s glossary of Terms”, available at www.vircom.com.

Visual codes in this document

For the sake of readability, this document has been laid out using visual marks to help the reader keep track of spammer comments and quotes from anti-spam experts. Here is a legend of the marks in use in this study:

- Virginia
  Spammer
- Matt
  Spammer
- Thomas
  Spammer
- Michael D. Osterman
  International spam expert
- Michael Gaudette
  Vircom spam expert
Acknowledgements

We would like to thank Virginia, Matt and Thomas for allowing us into their inner-circle and sharing some of their experiences. Their assistance in this study was invaluable.

Expert Analysis

This analysis would not have been possible without the views and opinions of Michael D. Osterman who contributed to this document.

Michael D. Osterman
President and founder
Osterman Research
www.ostermanresearch.com

The Spammers

Virginia
Virginia is a 19 year old University student from the North-East United States. She is a “rookie in the spam game” and has only been involved in spamming since November 2003. Virginia started spamming to earn a few extra dollars and to pay for her tuition and housing. Taking an analytical approach to her work, Virginia views her spamming in terms of “campaigns” and has created her unique artistic approach to spamming.

Matt
Matt is a 29 year old part-time spammer. He lives in California and has been spamming for 19 months. He is contracted from several adult sites to find new customers, as well as cater its existing customer base with special offers and promotions.

Thomas
Thomas is the seasoned spamming veteran amongst our three participants. He is in his late 20’s and has been spamming part-time for over 2 years. His years of experience have given him a unique view of the industry and its effects on business and consumers.

Starting up

How did you get involved in spamming?

“I was looking for a part-time job, something that would help me pay the bills and not occupy a lot of time. I was suffering from starving student syndrome big time… My friend mentioned doing this in passing to me, and the more I thought the more the job appealed to me. At first it seemed almost too good to be true, I had pretty much all of the hardware I needed all I had to do was invest in a new internet provider, and buy a list of e-mail addresses. I started up for pretty much nothing and turned a profit on the first day!”

Matt started spamming as a result of his affinity for hacking and computer security. Matt currently works in the computer industry in the Silicon-Valley, and uses his work experience to hone his spamming techniques.

“I have always been interested in the what’s of computing, what makes the anti-spam filters work, and then how I can bypass them. After a while I realized that I could make a few dollars from this.”

Thomas worked for a large multi-national corporation as a manager in IT for seven years before getting laid off in early 2002. As his own boss, spamming offered Thomas the freedom to pursue other goals while earning money. Currently he is only spamming part time, and has since taken on another full time job in the IT industry.

“I fell into it, because it was so cheap to start up, and I had plenty of time to spend with my kids.”

All of our spammers agree that one of the main reasons why they began spamming was because it had an extremely low start-up cost. Most spammers can get started for under $1,500.00 and may earn back their initial investment within a few days.
Making money

Does spam pay?
The image of a spammer’s income and the actuality are two different realities. It is widely held that the majority of spammers earn relatively little money while a small percentage of spammers earn the lion’s share.

How do spammers make money?
Spammers can earn money in a number of different methods:
- Sending spam to sell their product;
- Harvesting e-mail addresses;
- Joining affiliate programs.

Sending Spam to sell their product: Some spammers earn money by selling their own products or services. The types of commodities can include items such as pirated software or pornographic material; in general, a spammer looks for a product that is simple for the spammer to distribute to their customers.

Harvesting e-mail addresses: Spammers build lists of millions of names and sell these lists to other spammers. A spammer will pay a premium for lists that are categorized geographically, as well as authenticated “clean” lists, which means that the e-mail addresses listed have been validated.

Affiliate Programs: This is the most common type of spamming activity. Under an affiliate program, spammers are hired by companies who pay them based upon either:
1) The amount of leads they bring to the site (click through rate)
2) The sales generated from the spam (commission)

How much money do you make from your activities, on average?
“It varies, but I have made as little as $150 per campaign or as much as $2,000.00. It depends on the product, timing and my creativity.”

For Virginia, a campaign consists of an e-mail burst of approximately 5-days. Virginia explains that the 5-day period allows her to distribute the mail at least once or twice to the 40 million recipients in her database. In addition she estimates that she has a 5-day window in which to trick certain spam filters before a fix is introduced and released into the stream.

“That is pretty tough to know, it varies wildly. I calculated that I earned around $1,200.00 per week last year. The most I earned in a week was $6,500.00, and the least was $1.00, so I have done the gambit.

What type of products or services do you sell?
Like the majority of spammers, all of our participants work strictly through affiliate programs. They are paid either directly by the company they are representing or through intermediaries.

“I have strict rules regarding the types of products that I market. I will not market porn or stuff like that. I have been very successful with the low-carb diet plans. It is after Christmas and everyone wants to lose weight. I started this campaign the week another report made the rounds saying that obesity was a bigger killer than tobacco. My current campaign involves discount travel. So far it has been quite successful because of all the students going on spring break and people suffering from winter doldrums.”

“I have an exclusive contract with several adult sites, they have me advertise specials or other offers to its current list of subscribers and also to promote these sites to others.”

Matt works for an affiliate that manages 12 different adult sites. Part of Matt’s work is to promote all of the different sites to registered subscribers as well as any other person contained within his database of e-mail users. Matt is paid a commission for new subscribers, and spends the majority of his time trying to solicit new customers to his affiliate.

“I have peddled everything from diet pills to porn. I usually get the biggest response from porn... skin sells, unfortunately.”
How do you get your contracts?

“I work with a close knit group, who look out for each others’ interests. All of my campaigns were a direct result of contracts that I got from the group.”

“I get most of my contracts through word-of-mouth. I don’t work in an industry where you can really advertise yourself. Between friends and satisfied customers, I am almost always assured a contract.”

Organization

Is the spammer community a close-knit group?
Virginia and Thomas are members of a loosely formed ‘spam gang’ of 4 spammers. They share lists, leads, and information regarding affiliates and opportunities. Because Matt is under contract with a group of adult sites, he presently does not belong to a ‘spam-gang,’ even though he has worked with Thomas in the past.

“I have met some very smart and talented people who are spammers. I work a lot with Thomas and he has showed me a great deal.”

“Not really, it is not like seeing people at the water fountain during smoking breaks. You communicate through e-mails or chat online. I have never personally met a fellow spammer, nor talked to any on the phone.”

“Close-knit is not the best way to describe the spammer community. I am pretty aware of all the major players, but I can’t say that I am close to any. You work in groups because it is a necessity, but when it comes down to it, it is every one for themselves.”

What are hot topics for you now?
Timing of the spam message is critical to the success of the spammer’s campaign. Affiliates hire spammers at particular times of year to market their product or service knowing that the timing of the spam will ensure higher sales, for example: New Years will see significant increases in spam dedicated towards diet aids, as well as low interest loans to pay off the bills from the holiday season.

“Without a doubt Paris Hilton and Janet Jackson, sex sells and as long as you give the consumer a window to peak into the seedier side of celebrities’ life, it will continue to sell. Before you would have to go to the video store and sneak behind the curtain to look at the adult films, now it is just a click away.”

“Tax software, it is the time of year when people are looking to do their taxes.”

Harvesting

How spammers get e-mail addresses
For spammers, the most important item is their database of e-mail addresses because these e-mail lists can be used for spamming purposes, sold, or exchanged for other lists. Spammers have several weapons in their arsenal to acquire e-mail addresses:

Harvesting software (also known as spiders, bots, robots and crawlers): Spammers and harvesters use these tools to search the internet for e-mail addresses for the purpose of spamming, selling, or swapping. Within a very short period of time, a good e-mail harvester can harvest millions of addresses.

As e-mail harvesters search the internet they look for the @ symbol that is the essential part of all e-mail addresses. E-mail harvesters can find addresses from a variety of sources on the internet including:

- Web pages
- Newsgroups and forums
- Compromised Mailing lists
- Chat rooms and IRC
- Unsecured opt-in lists
- Corporate web pages
- Web-based surveys
- Web-based order forms

— You work in groups because it is a necessity, but when it comes down to it, it is every one for themselves.
How spammers get e-mail addresses:
- Mailing/opt-in lists
- Opt-out methods
- Viruses, spyware, malicious code
- Dictionary/phone book attacks
- Social engineering

Mailing / Opt-in Lists - Anytime consumers subscribe to any mailing or opt-in list, they run the risk of having their e-mail address compromised by spammers. In certain cases some legitimate and highly respected companies have sold lists of their subscribers to other companies, who in turn sold it to others.

Opt-out methods - Many spammers will use op-out methods to gather and verify lists of e-mail addresses. When consumers respond to unsolicited e-mails by clicking on attached links, or replying to opt-out, in many circumstances they are simply confirming that their e-mail address is valid and accurate to the spammer.

Viruses, Spyware, Malicious Code - Viruses and spyware have been used recently by spammers to extract the contents of a computer’s address book. Viruses have also been written (Trojans) for the purpose of making infected systems relay slaves so that they become platforms to distribute spam.

Dictionary / Phone Book Attacks - A common harvesting tactic that consists of automatically requesting likely e-mail addresses to a server by combining letters and numbers in an attempt to find, or validate, active e-mail addresses, for example: johnsmith@domain.com, john.smith@domain.com, john_smith@domain.com, jsmith@domain.com. Spammer’s are using this technique less frequently because it results in very poor lists.

Social Engineering - has emerged as an effective spammer’s tool to validate and harvest e-mail addresses. A spammer will send out millions of e-mails in an attempt to motivate the recipient to respond. The tricks and hoaxes the spammers use vary from the recipient winning a contest to the recipient being told that they are being charged for an item that they never purchased. No matter what the method is, the goal is the same - to get the recipient of the e-mail to answer, therefore validating their address.

How do you get your e-mail lists?

“I bought my first list from the friend who introduced me to spamming for $100.00; this was a pretty good deal because it had over 15 million names on it. I used this list to swap for more lists, now I have over 40 million names in my database.”

“I bought my first list over the net and it was a pretty pathetic one that had made its rounds over and over again, I doubt more than 10% of the addresses were valid. Since then I have used a crawler in the past, but I found it was too much work and I did not like the results I was getting.”

Currently, Matt gets most of his addresses from the affiliates that he works for. He considers these lists as cash cows because once he finishes his work with the affiliates he can sell the lists for a profit as well as use them for any other contracts he gets. The affiliates acquire the lists through registered users.

“Your lists are your livelihood, my lists are even more valuable than most because I have ones that people subscribe to, therefore they are valid and I can cater my messages to their needs.”

“I have bought lists in the past, but mainly I trade for them now. The most I ever paid for a list was $899.00. This was a list of 4 million clean (valid) e-mail addresses in Washington, Oregon, California and Nevada. The first time I used this list I generated over $2,500.00 in commissions.

What is the most time-consuming aspect for you?

Once a spammer has a list of e-mail addresses they must conceptualize, create and distribute a message that will not only attract the recipient’s attention and possibly generate a sale, but must also deceive any spam filters that are implemented to eliminate the spam.

“I try to be as creative as possible with the look and the feel of my work. I would love if I could create messages that would read like a print advertisement, but I know better; either it would be too large or a spam filter would catch it.”

“Maintaining a database, making sure all of my e-mail addresses are up to date occupies a great deal of time.”

“I spend more time on the subject line than on the body of the message. The subject line is what will draw in the customer initially. Testing the message to have it get past spam filters takes a lot of patients, because if you can not get past the spam filter, then you need to figure out why it did not get through.”
Spam tricks

What are some of the techniques that you use?

Our participants were hesitant to reveal the majority of the tricks they use. However, they did talk about some of the techniques that they have used or are familiar with. In order to explain some of our spammer’s techniques, we consulted with Michael Gaudette. As the product manager for Vircom’s Modus line of anti-spam solutions, Gaudette has a thorough knowledge of the techniques used by spammers to circumvent spam filters. He constantly monitors spam traffic, not only to learn the techniques of spammers but also to help create solutions that will prevent spam from occurring.

Technique: Top-to-bottom HTML Coding

“When I create new campaigns, there are 2 crucial factors that I all look at; the flow of the message and will it get past a spam filter. The message itself has to attract the reader and compel them to buy, but it must be put in a format that will arrive to its intended receiver. I like using HTML, it is more attractive than just plain text, and you can code the tables in such a way as to make them impervious to spam filters, for example coding from top-to-bottom.”

Michael Gaudette: “Using a table in this manner involves coding words as individual letters that are coded in HTML from top-to-bottom (B S t o) but read left-to-right by the recipient. This technique is very difficult for some anti-spam filters to detect because they do not identify individual words like “buy” or “Save all they read is gibberish.”

Virginia also discussed several other techniques that she has come across or used.

Technique: Zero font size

Michael Gaudette: “This technique allows the spammer to disguise the message by having the message read as individual letters with a spacing between the letters, because the font size for the spacing is 0 the letters read as normal words, but most anti-spam filters have difficult times reading them.”

NOTE. The zero font size has been illustrated in red here but would normally be invisible to the reader.

Technique: HTML numbers instead of letters

Michael Gaudette: “This technique allows the spammer to disguise the message within a series of ASCII codes.”

```
BUY Now and
Save Two for
The Price of
One
```

Technique: Embedded Image

“I have created HTML messages consisting of just an image”

Michael Gaudette: “Because the text message is embedded within the image, this technique attempts to trick spam filters by eliminating text as a method to detect spam.”

“I have several great techniques that I am not going to tell you, but I can say that I can get by any spam filter.”

Thomas has also used techniques which he no longer considers as effective techniques to combat spam filters.

Technique: Added spaces or characters

Michael Gaudette: “This is a very simple technique that spammers use to attempt to trick spam filters. A spammer simply places an empty space or some type of character like a - or * between...
key words. B U Y or B-U-Y or B*U*Y. Most spam filters will search the body and header of a message looking certain keywords or phrases. This technique tries to fool the filter by disguising the word.”

**Technique: Misspelling**

Michael Gaudette: “Like placing spaces and adding characters between letters in words, the goal behind this technique is the same; it is to fool the spam filter by making it difficult for the spam filter to distinguish words or phrases.

Spammers frequently replace the letter ‘I’ with the number ‘1’ (one), or the letter ‘O’ with a ‘0’ (zero), or add international language accents to the letters. It is very easy to do, but not that effective.”

BUY NØw a n d $ a v é T w o f o r t h e p r i c é o f w o n

**Technique: Hashing**

Both Virginia and Thomas have also used a technique known as hashing.

Michael Gaudette: “This is a very common technique used by a lot of spammers to attempt to trick spam filters. Hashing works as follows:

A legitimate message is created with the text and background the same color or very similar colors (white on white, black on black) a short spam message is added in a contrasting text color (black text on a white background, or white text on a black background). The results being that the recipient only sees the spam message.

It is absolutely impossible to embrace the extent of difference there is between traditional and modern China when you first get out of the airport and ride towards the city. How can I explain this? You’re looking through the cab’s window, searching for something your eyes can focus on. Buy Now and Save Two for the price of one

But as you get closer to the center of the city, you start to notice difference after difference, so fast in fact that, before you know it; you’re downtown, feeling like you are riding a flying cab in Blade Runner. Speeding along a neon-lit highway between skyscrapers with multiple-story, rainbow-colored advertisements, you ask yourself where the hell can the pagodes, zen garden and tai-chi adepts have gone.

**How do you make sure that your messages get through?**

“I test on the spam filter in my father’s office, if I can get through it, then I can get through most spam filters.”

“I use two spam filters, one is open source that I downloaded for free, and the other is an enterprise copy of a commercial filter.”

Michael Gaudette: “For a spammer, the click through rate is usually very, very low, so it is volume that counts. In order to maximize the amount of messages that get through to their prospective customers, most spammers test on one or more spam filters.

One thing that should be pointed out though is that if a spam message can circumvent one spam filter, it does not necessarily mean that it can get through all spam filters. Different spam filters have different capabilities; some spam filters can only catch 50% or 60% of spam, while some of the better ones catch more than 95% of spam. Vircom’s Modus solutions are among the highest at 98.2%”
What do you think of spam filters?

“Spam filters give you a sense of false self-confidence. They can work very well, but when they catch important documents that you need, then they can do a lot of damage.”

“There is no doubt that they have made our job more difficult, but I have never come across a spam filter that I could not get around if I tried.”

How do you remain undetected by ISPs?

In order to distribute e-mails in such great quantity undetected from Internet Service Providers (ISPs) many spammers will use different techniques including: hijacking third party unprotected servers and using them as platforms to spam, or by sending spam through different ISPs.

Our participants were reluctant to discuss the methods that they use to distribute their e-mails. Most methods used by spammers to distribute their bulk e-mail are illegal, and none of our participants wished to incriminate themselves by admitting to any illegal activities.

“I send out short bursts on numerous machines to stay under the ISP wire”

Virginia has used a technique where she sends out bursts of 100 messages every 20 seconds from approximately 6 different computers using different ISPs. In a 12-hour time span, she averages over 1.3 million messages.

Legislation

Will the anti-spam laws have any bearing on your work?

On January 1, 2004, The United States enacted legislation designed to curb the flood of spam. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) established a nationwide law governing e-mail spam.

“Not at all.”

“I do not think that it will have any effect in the short run, it is a little convoluted, it is untested, and the reality is who will bother enforcing it. The price it would cost to prosecute a spammer is a lot more than the cost of spamming.”

Thomas emphasized that because of its limitations CAN-SPAM has been a detriment to all types of e-mail marketing.

“Since it [CAN-SPAM] came into effect some “legitimate” e-mail marketers have also got into trouble. People constantly forget what they have subscribed to, or they do not trust the opt-out system, or for a hundred other reasons, they report this as spam, then the marketers must prove that this person subscribed. The whole thing is a big mess.”

“Right now, the US government has had zero results in controlling spam. Perhaps if they review some of its problems then it will have an effect.”

As a method to get consumers onto the site of his affiliates, Matt uses the opt-out solution to require the recipient to go to a page on the affiliate’s website and look for an opt-out option.

“When people want to opt-out, they must come onto the site, and search for the right opt-out option. I usually take them off my list, but I know others who use this to legitimize the e-mail address and continue to spam them.”

Opt-Out Solution

One of the most controversial issues regarding the CAN-SPAM act is the requirement for a viable opt-out mechanism in every message. The big concern regarding the opt-out mechanism is that it gives spammers the right to spam. It also enables spammers to send spam until the recipient asks them to stop. Furthermore, it leaves to spammers the responsibility of dictating which steps recipients must take to get off their mailing lists. For recipients, this might mean:

“...because of its limitations CAN-SPAM has been a detriment to all types of e-mail marketing.
Spammers on spam

The concern about spam is well-founded. Spam is estimated to make up over 65 percent of all e-mail traffic today, perplexing and harassing consumers, enterprises, internet service providers, and legitimate e-mail marketers alike.

“E-mail has become the major delivery mechanism for marketing material simply because of dollars and cents,” says Michael D. Osterman. “Whereas other marketing strategies like bulk mail involve costs to create, produce and send the material, the cost of sending spam is virtually non-existent.”

What are the costs to the public from spam?

“I know that people get frustrated by spam but I don’t think it deserves all of the press it has received lately.

“Nothing.”

“If a person does not like the e-mails they receive they can simply erase them or buy a filter.”

“You cannot look at spam as a simple nuisance, because it is a burden on everyone: Loss of productivity, increased bandwidth consumption, the need for additional hardware and spam filters are all associated directly with spam. We have estimated that the economic cost of spam is $1,400.00 a year for every enterprise e-mail user. For a company of only 10 employees that amounts to an additional cost of $14,000.00 per year all due to spam.

Do you worry about who gets your messages?

For all of our participants, this question brought the most animated discussion. The possibility of children being exposed to certain types of messages weighed upon all of the participants, but they all maintain a distant, almost detached outlook regarding the recipients of their messages.

“Definitely, that is why I will never market porn.”

“None of us can really say that our messages are not opened and read by children. I have peddled flesh in the past, and will do it again. I am not going to lie and say that I am above that. The fact is that skin sells!”

Matt later justified his answer by stating that the recipients of his adult oriented material were all registered members for these sites.

“When you [spam], you do not look at the names in your database as individuals, you have millions of them.”

What do you do with the spam that you get?

“I look at spam differently than most; I look at how the person created it, what their thought processes were. I critique it and learn from it. The greatest way for a (spammer) to learn the tricks of the trade is to study the work of others. Some are brilliant, while others are just stupid.”

“I delete them 1-2-3, I do not believe for a minute that spam is so destructive, and I do not get that much either at work or at home.”

“I use a spam filter so I receive very few”.

Do you ever get complaints?

“Sometimes, but I never read them.”
“All the time, I have had my life threatened several times. I have been called every name in the book… hey you just have to shake it off.”

“Never, but I assume that some of the servers I have used have received complaints. A good spammer is not traceable.”

Would you buy a product from an e-mail campaign?

“It depends on the product, but yes there are some very good bargains, from very reputable firms.”

“For sexual material, I would because it is more or less anonymous. It beats making eye contact with the clerk at the video store.”

“Are you kidding? No way!”

Do you consider what you are doing as illegal?

“No way!”

“Not at all, we are marketing and promoting items that large companies, fortune 500's in many instances pay us to market. It is typical big business, they go after the little guy but let the big businesses off the hook.”

“Illegal - no. A pain in the […] - yes”

How long will you continue to spam?

“I think by the summer I will have earned enough money, so most likely I will stop then.”

“When I either get arrested, or until porn stops selling. In other words - No time soon!”

“It is getting tougher for us small fry. I would be surprised if I last a year. ISPs are getting smarter, anti-spam filters are getting better, affiliates are running scared.”

Can Spam ever be controlled?

“I think there is enough outrage right now that they will have to do something about spam. I just don’t know what. Spam filters are flawed and can do as much harm as good. The laws are wimpy and do not work either.”

“As long as people can make money from it, then nothing will happen. It needs to be regulated, and set up like any other business.”

“I doubt it! Spam will always be around in one form or another. You may see it peak then slowly decline, but it is the only way right now to get millions of messages out.”

“Over the last year, you can see a decline in the amount of affiliates hiring us to market their products. If it becomes unprofitable for the companies who hire us because they are being sued or they are being associated as a company that supports spam, then I can definitely see spam slow down.”

“The only answer to controlling spam is to fight spammers with the same weapon they use: Technology. To control spam, it must be rendered economically non-viable. Now that is difficult to achieve because it costs virtually nothing to send. However, if we can increase the cost of sending a spam message, we can make it non-viable and the only way we can do that is through the increased use of anti-spam tools.”

When anti-spam filters are effective, they can eliminate 95% or more of the incoming spam. Michael D. Osterman illustrates how this can make the spam message non-viable - “...If an anti-spam filter can stop 95% of the spam that reaches an end user, the cost to the spammer of reaching that potential customer has risen by 20 times. Increasing the effectiveness of these filters to 97% increases the cost to the spammer by 33 times. The hope is that the potential revenue available to spammers drops by a corresponding amount and equilibrium is reached.”
Finally, any myth about spammers you would like to clarify?

“We’re not horrible people; we are earning a livelihood like everyone else. I wish people could appreciate just how hard it is to properly create an effective marketing message.”

We are just earning a living.*

We are not all parasites. Most are but not all of us.”