



# How Much eMail Can You Afford To Lose ?

**Atlanta Tech-Security Conference  
November 29, 2007**

# Today's Story...

- There are lots of products that try to fight email spam
  - And some anti-spam “filters” actually do an OK job
- But, losing legitimate email during the fight is a disaster
  - And EVERY anti-spam “filter” loses email
- Let's explore why we have these problems
- Then, we will discuss a real solution

# Thesis: eMail Integrity

- Deleting spam from your Inbox is an annoyance
- Losing legitimate messages while trying to block spam is a disaster
- Spamming is a criminal business
  - Not going away
  - Volume and frequency of attacks are increasing
- Businesses rely on email to drive relationships and revenue
  - They must be sure that information is getting through
  - eMail Integrity: Communications you can count on

# Recognition: Product of the Year



In Nov 06, Government Computer News tested the I.C.E. Box in their labs

*"The I.C.E. Box offers a far better way to eliminate spam from your network than any filtering appliance we have ever tested. It took on a billion spam-laden e-mails and destroyed them all, and without generating any false positives."*

*"... one product that not only was the best in its class, but one that might just be on the forefront of change for an entire industry."*

*"...the best of the best for 2006, earning the I.C.E. Box the ultimate Reviewer's Choice award."*

# The Opening Question:

---

Why haven't we stopped spam ?

# Two Reasons

---

1. Started from a flawed misconception
2. Spammers are making real money and are highly motivated to keep evolving

# Let's review: 29 Years Ago...

...the first spam message was sent across the Internet



# 29 Years Later...

...you are still trying  
to FILTER the spam  
out of your Inbox



# The Risks from Spam are Now Enormous

More than just an annoyance for users...



Spam delivers malicious threats from professional criminals

# ...Along With the Risks from Using the Filters



You've  
**Got** Mail

Legitimate business  
lost in the junk  
folders

You can no longer trust your  
most important business tool

# Misconception: Spam “Filters” Will Never Work

The root problem that spam filters can never overcome is that they are just “guessing machines”



No context: just “analyzing” words, phrases and patterns

Paradox: greater sensitivity = more “false positives”

But, not all “bad words” are bad

Spammers keep adapting

# The Driving Question:

---

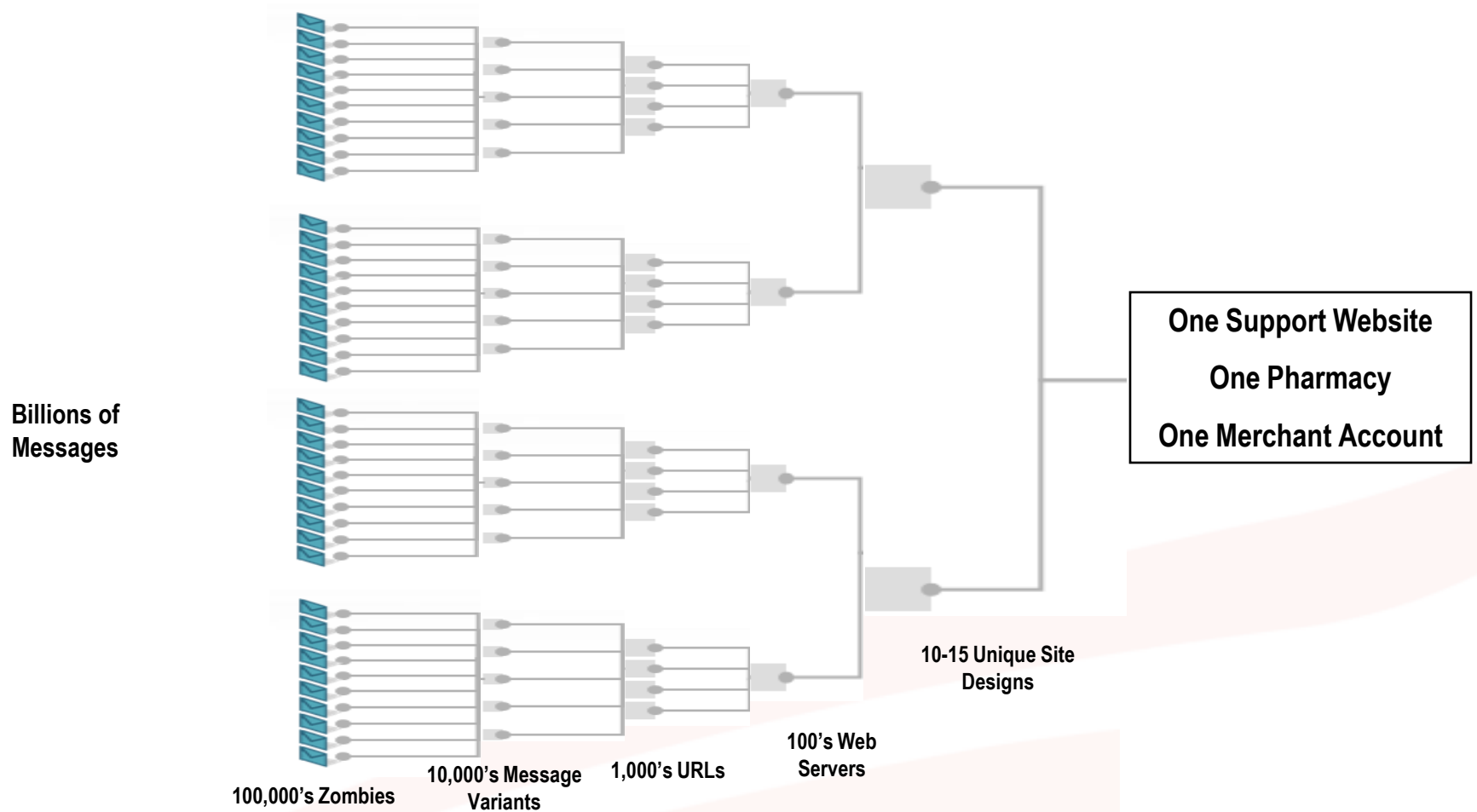
Why haven't we stopped spam ?

Why do spammers spam ?

# Anatomy of a Spam Attack

- Spam content
  - 1.5 billion messages over 2 weeks in Mar 07
  - ~2000 unique content mutations (changed every 12 minutes)
  - 1500 unique domains used (changed every 15 minutes)
- Spam source
  - 100,000 infected PCs (zombies) in 119 countries
- Command and control (C&C) infrastructure
  - Web sites, Web servers, DNS servers, payment processing and customer service systems
- Criminal
  - Single pharmaceutical store processed all orders

# Identifying the Command & Control



# Multiple Online Storefronts

Home [FAQ](#) [About](#) [View Cart](#) [Customer Support](#) [Contact Us](#)


## Pharma Shop

**World Wide Shipping**

Save up to 80%


- Discreet Packaging
- Cheapest Generic Medication
- Worldwide shipping
- Buy in Bulk and Save

**Feature Product**




Cialis 

Today we have a special on our products.

[BUY](#)



**Hot Weekly Specials**

Levitra 	\$99.00	<a href="#">BUY</a>
Viagra 	\$74.00	<a href="#">BUY</a>
Cialis 	\$96.00	<a href="#">BUY</a>

**HOT weekly specials**

**Xanax**

30 x 1.0mg Xanax (Alprazolam)

**ONLY \$130.00**

[BUY](#)

**Soma**

80 x 350.0mg Soma (Carisoprodol)

**ONLY \$79.00**

[BUY](#)

**Levitra**

10 x 20.0mg Levitra (Vardenafil)

**ONLY \$99.00**

[BUY](#)

**Ambien**

30 x 10.0mg Ambien (Zolpidem)

**ONLY \$145.00**

[BUY](#)

**Valium**

30 x 10.0mg Valium (Diazepam)

**ONLY \$155.00**

[BUY](#)

**Cialis**

10 x 20.0mg Cialis (Tadalafil)

**ONLY \$96.00**

[BUY](#)

**Cialis**

10 x 20.0mg Cialis Soft Tabs

**ONLY \$79.95**

[BUY](#)

**Viagra**

4 x 100.0mg Viagra (Sildenafil Citrate)

**ONLY \$74.00**

[BUY](#)

**Ultram**

60 x 50.0mg Ultram (Tramadol)

**ONLY \$85.00**

[BUY](#)

**Men's health**

- Cialis (Tadalafil)
- Cialis Soft Tabs
- Levitra (Vardenafil)
- Viagra (Sildenafil Citrate)
- Viagra Gel (Sildenafil Citrate)
- Viagra Soft Tabs

**Anti Depression**

- Ativan (Lorazepam)
- Effexor XR
- Paxil (Paroxetine Hcl)
- Prozac (Fluoxetine)
- Valium (Diazepam)
- Xanax (Alprazolam)
- Zoloft (Sertraline)

**Pain Relief**

- Ultram (Tramadol)

**Sleep**

- Ambien (Zolpidem)

**Muscle Relaxants**

- Soma (Carisoprodol)

**Weight Loss**

- Meridia (Sibutramine)
- Phentermine (Generic Meridia 10mg)

**Antibiotic**

- Cipro (Ciprofloxacin)

MyCanadianPharmacy

ALL PRODUCTS LIST [HOW TO ORDER](#) [ABOUT US](#) [CUSTOMER SERVICE](#) [CONTACT US](#)

## Erection Pack

10 PILLS CIALIS + 10 PILLS VIAGRA + FREE SHIPPING

Try our SPECIAL ERECTION PACK! Two best ED medications in one super pack. Lowest price and FREE shipping. Time limited offer - valid 10 9th of June only!

**\$129.99 ONLY** [ORDER NOW](#)

**PRODUCTS LIST**  [SEARCH](#)

**Men's Health**

- Cialis Soft Tabs [Details](#)
- Viagra Professional [Details](#)
- Viagra Soft Tabs [Details](#)
- Cialis [Details](#)
- Generic Viagra [Details](#)
- Levitra [Details](#)
- Maxman
- Flomax
- [view all products](#)

**Anti-Depressants / Anti-Anxiety**

- Wellbutrin SR
- [view all products](#)

**Pain Relief / Muscle Relaxants**

- Intrex
- [view all products](#)

**General Health**

- Human Growth Hormone [Details](#)
- 100% Pure Okinawan Coral Calcium
- Quick detox
- Cinacrol
- [view all products](#)

**Weight Loss**

- Pure Natural Hoodia
- Premium Diet Patch
- Liposafe
- Lipothin
- [view all products](#)

**MOST POPULAR PRODUCTS**

**Cialis Soft Tabs as low as \$5.78**

Just like regular Cialis but specially formulated, these pills are soft and dissolvable under the tongue. The effect of this is more direct absorption into the bloodstream, rather than through the stomach. Result - a powerful, lasting effect of up to 36 hours.

[more info](#) [order now](#)

**Viagra Professional as low as \$4.07**

Viagra is a prescription drug used to treat erection difficulties, such as erectile dysfunction (ED).

[more info](#) [order now](#)

**Viagra Soft Tabs as low as \$4.1**

Viagra Soft Tabs are mild flavored soft tablets for the treatment of male erectile dysfunction. They are equivalent to regular Viagra, however due to their soft formulation, they are absorbed directly into the bloodstream. As such, they contain a much smaller dosage of Sildenafil Citrate to achieve the same result.

[more info](#) [order now](#)

**Cialis as low as \$5.07**

Cialis, or Super Viagra, is used to treat erectile dysfunction, more commonly known as impotence. A man is impotent if he cannot achieve or sustain an erect penis for sexual activity.

[more info](#) [order now](#)

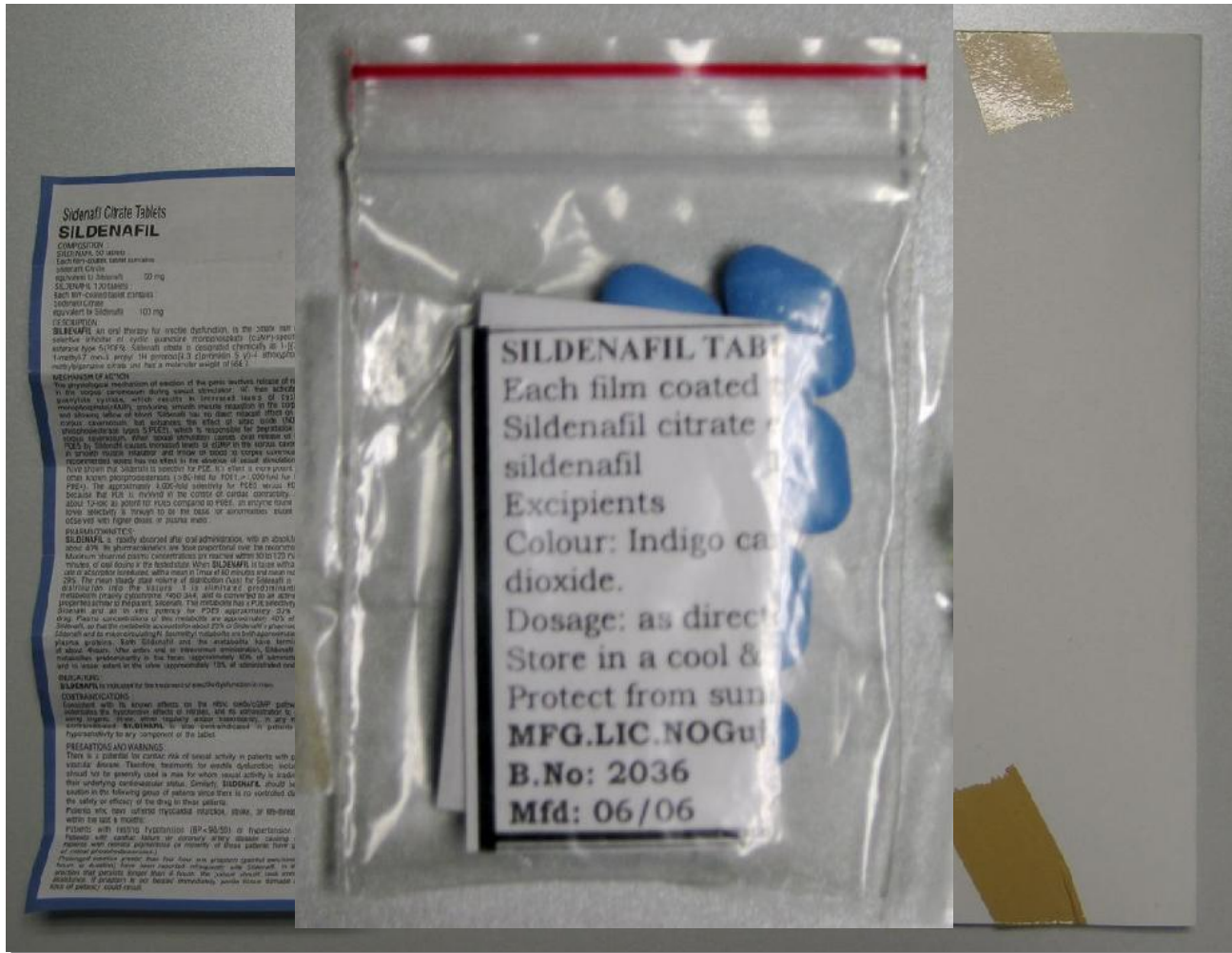
**Generic Viagra as low as \$3.5**

Generic Viagra, called Sildenafil

# Physical Address of My Canadian Pharmacy



# The Merchandise Arrives



In 14 orders, all were counterfeit and only 2 actually contained Sildenafil.

The others were just “pill binder”.

# Motivation

---

It has been widely reported that the *My Canadian Pharmacy* site generates over \$200M per year

# Another Spam Attack

Wed 22 Aug 07



## MySpace brought down a spammer

- 11,000 similar MySpace profiles and 11,383 unique America Online email accounts to register those profiles
- MySpace asserted that the defendant sent nearly 400,000 messages and posted 890,000 comments from 320,000 hijacked MySpace user accounts
- MySpace also claimed that the defendant created groups on MySpace that redirected users to the defendant's Web sites, which included altering the MySpace "unsubscribe" link to point to the defendant's Web sites instead of actually allowing members to unsubscribe
- The defendant admitted his Internet business earns him about \$1 million per year.

# The Business Question:

---

Why haven't we stopped spam ?

Why do spammers spam ?

**Does spam really impact my business ?**

# The Latest News



[Back to Story - Help](#)

## Overzealous Spam Filter Proves Costly for Lawyers



Robert McMillan, IDG News Service

Thu Jul 12, 5:00 PM ET

The trouble at Franklin D. Azar & Associates PC began with pornographic spam.

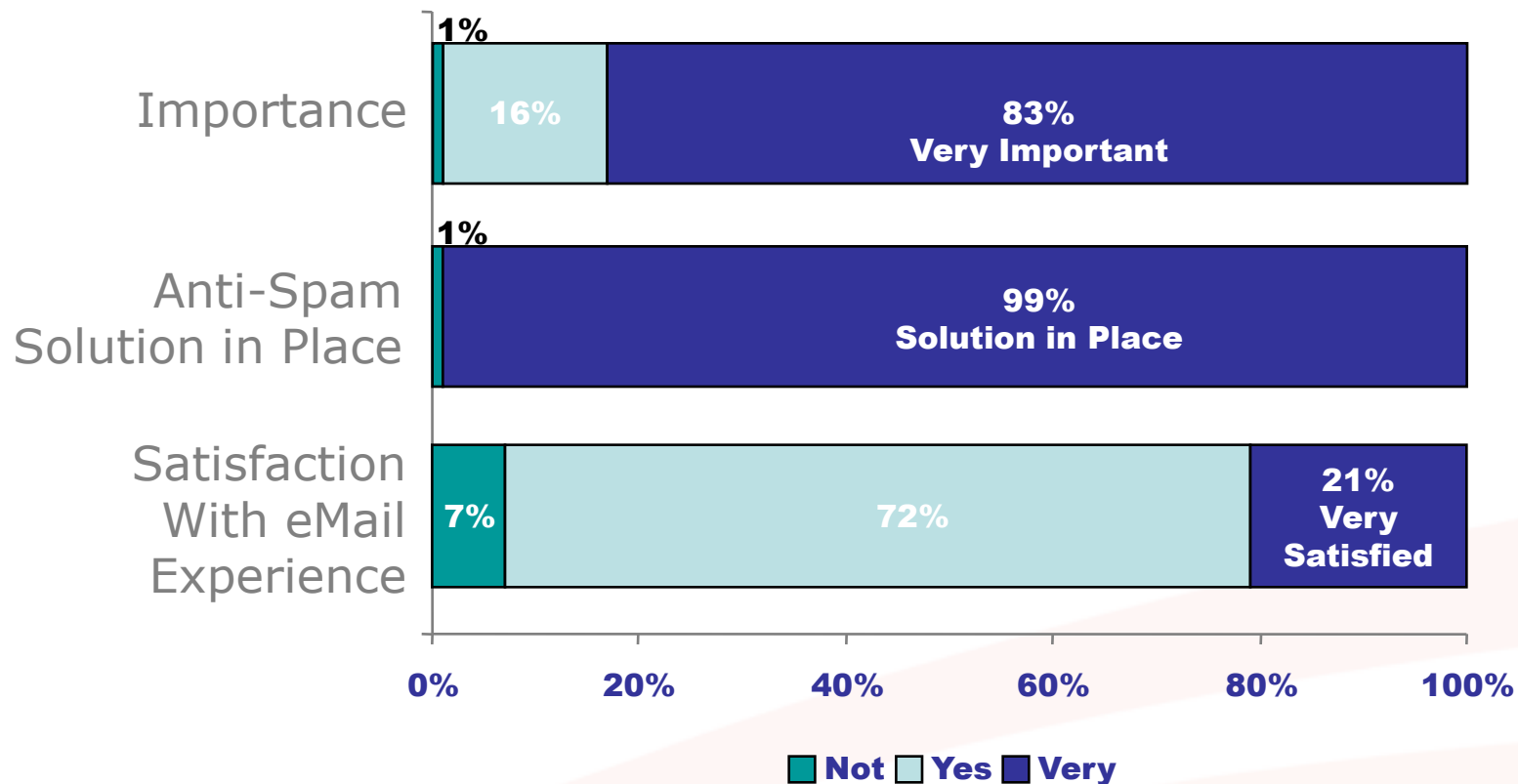
Last May the Aurora, Colorado, law firm was being bombarded with offensive messages, and enough of it was seeping through the company's spam filters that employees complained to management, and IT administrator Kevin Rea was told to do something.

What happened next, as detailed in federal court filings, shows how the fight against spammers can backfire. Spammers have been using increasingly sophisticated techniques to evade filters, so that over the past few years and despite predictions to the contrary, unsolicited e-mail continues to plague businesses worldwide.

On the morning of May 21, Rea dialed up the spam settings on the Barracuda Spam Firewall 200 Azar & Associates was using to block unwanted mail. The changes made it harder for spam to land on the desktops of company employees but they also had one unforeseen consequence: the Barracuda Networks Inc. appliance began blocking e-mail from the United States District Court for the District of Colorado, including a notice advising company lawyers of a May 30 hearing in a civil lawsuit.

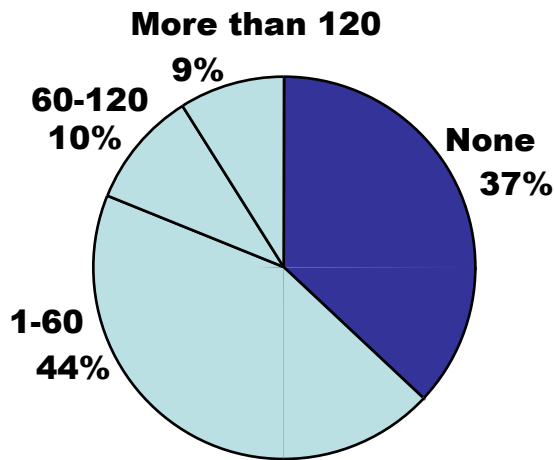
# User Satisfaction “Gap”

## eMail is Very Important To Business Success



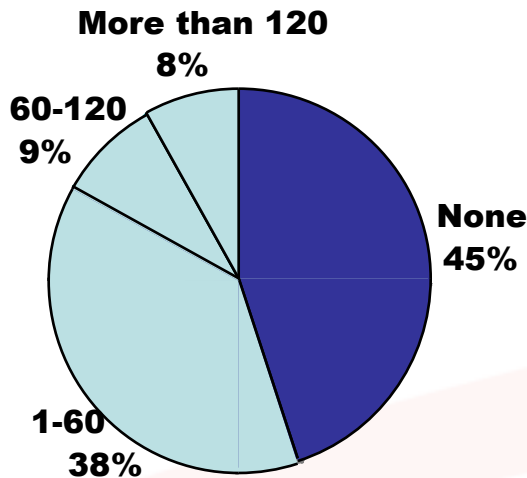
# Ineffective Anti-Spam Products are Worse Than the “Nuisance”

Have you ever been asked to resend an email?



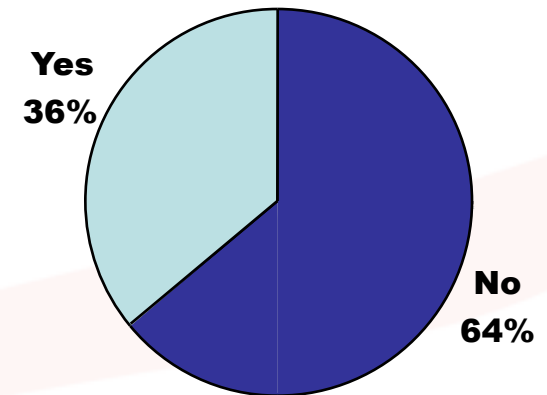
Average 44/year

Have you ever had messages get trapped in a filter?



Average 40/year

Have you ever lost business because email did NOT arrive?



# The “Value” of eMail

In a survey of over 500 business professionals:

What is the value of the most important email you ever received ?

Answer: >\$12 million (average)

>\$8 million (without the 2 >\$1B aerospace company answers)

What if that was the message that got lost ?

# So, The Last Question:

---

Why haven't we stopped spam ?

Why do spammers spam ?

Does spam really impact my business ?

**How much email can you afford to lose ?**

# But What About Spam

- What is “spam” ?
- Unsolicited commercial email
  - [www.antispam.govt.nz](http://www.antispam.govt.nz)
- Unsolicited bulk email
  - wikipedia
- Unsolicited bulk anonymous email
  - Sendio

eCard w/  
embedded bot

Warranty recall  
message

# The Spam Triad



Simply “unwanted” email is not spam

# Really Solving the Problem

- The problem isn't "getting spam"
  - it's "getting what you really want"
- When the first Sendio I.C.E Box shipped in Jan 2004, it was based on a simple premise:

With email, "what you want" is based on the message sender and not the message content

# Your “Relationship” with the Sender

- Are you someone I want to communicate with ?

▪ Are you who you say you are ?

- If so, then I should get all of your messages, unless...

Does the message contain “malware” ?

# So, Break the Problem Into Pieces

---

- First, is there any reason to ever accept an anonymous email ?
  
  
  
  
  
  
  
  
  
  
- So, if we block everything that is anonymous, what are we left with ?

# Identify “Unwanted”

- Is it acceptable to involve the participants in the process ?
- Of course !!
- Who else can identify “unwanted” ?

# What is eMail Integrity ?

All of the messages you want and none that you don't

- Effective / reliable / secure

## Validation

- Reputation
- Authentication

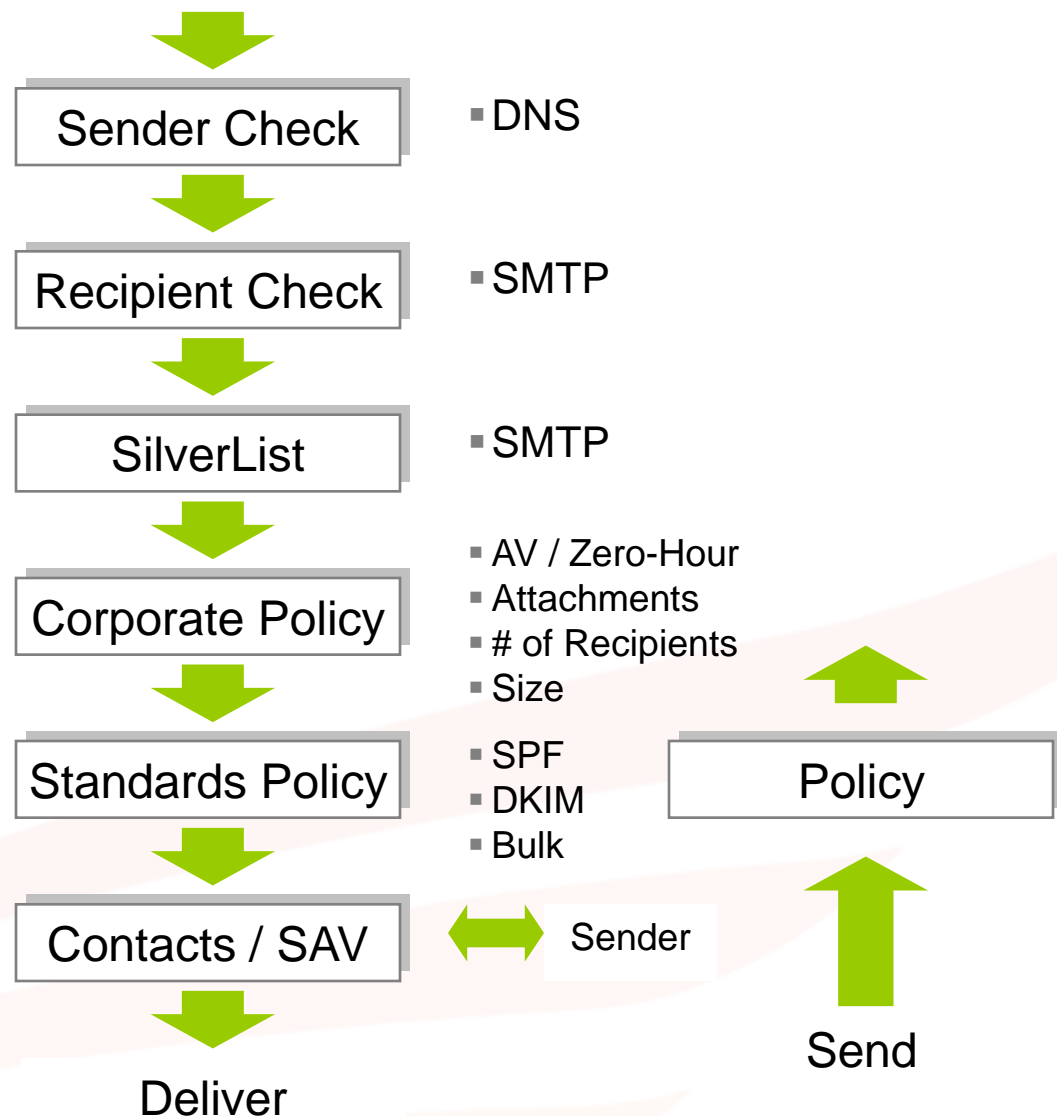
+

## Hygiene

- Anti-Virus
- Anti-Phishing
- Anti-...

# Sendio eMail Integrity Workflow

- The Sendio™ I.C.E. Box **integrates standards** such as Domain Keys and Sender Policy Framework with detailed SMTP protocol checks and Sender Address Verification (SAV) to **determine sender authentication and reputation**, instead of “guessing” about message content



# The Sendio™ I.C.E. Box Services Appliance

- Blocks 100% of spam
- Never loses an email
- Gives users control over what messages get into their Inbox
- Minimal administration time
- Complete anti-virus protection
- Inbound and outbound management
- Pays for itself almost immediately



**eMail Integrity: eMail Communications You Can Count On**

# I.C.E. Box Feature Overview

- A 1U turn-key service appliance
- 1 hr installation
- Minimal on-going administration
- Signature-based and Zero-Hour anti-virus protection
- Inbound & Outbound security
- Auto-Update
- Comprehensive reporting
- Scales from hundreds of users to tens of thousands
- Upload contact lists
- Evaluate with a pilot group
- Flash-based User and Admin GUIs
- Phased roll-out



# Flash-based GUI

Sendio I.C.E. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://ibx.sendio.com/sendio/ice/ui/

Headlines News CNET GP MapQuest Maps AA Expedia Wikipedia NetSuite AdWords XO MyFax Sendio Sandbox ProjectPath Sendio IBX GoToWebinar Sendio ICE House

**Sendio I.C.E.** Logged in as Tim Lee-Thorp

User

- Messages
- Contacts
- Account Info
- Logout

Admin

Copyright 2007 Sendio, Inc. 4.1.20070913.2-qa

Transferring data from ibx.sendio.com...

Inbound Messages Outbound Messages

Refresh View... Actions...

Messages 1 to 20 of 20 (found)

			Subject	Date	Size
	1	Pending messages, no bulk (DEFAULT)			
	2	Pending messages, show bulk			
	3	Delivered messages			
	4	Dropped messages			
	5	Rejected messages			
	6	SAV Response messages			
	7	ALL messages			
	8	Custom message search...			
	9	IDG Connect	IDG Connect's Tech Tuesday	9/18/07 5:28 AM	11 KB
	10	Budget Confirmations	Budget Rental Confirmation - Tue, Sep 18, 2007	9/17/07 2:46 PM	37 KB
	11	IDG Connect	<FRIDAY>	9/14/07 4:30 AM	11 KB
	12	Kathy Tomasino	Business Wire Announces Expanded Feature To	9/13/07 10:17 AM	884 KB
	13	Kathy Tomasino	Business Wire Announces Expanded Feature To	9/13/07 10:17 AM	884 KB
	14	Realtime Publishers Technol	Series Spotlight: Messaging and Web Security, \	9/12/07 12:52 PM	9 KB
	15	Products Guide	IMPORTANT - Send your nominations for 2008 Hi	9/12/07 12:08 PM	18 KB
	16	IDG Connect	IDG Connect's Tech Tuesday	9/11/07 8:09 AM	12 KB
	17	CMP Media	Take Our Survey on Media Usage - Enter to win	9/10/07 12:05 PM	4 KB
	18	Products Guide	LAST CHANCE TO NOMINATE - Who will win the ?	9/10/07 9:48 AM	18 KB
	19	IDG Connect	<FRIDAY>	9/7/07 5:10 PM	11 KB
	20	CIO Marketing	New Opportunities From CIO Magazine	9/6/07 3:43 PM	16 KB
	21	lotfi@ncsi.com	Naples, Vicenza and Aviano Exhibit Opportunit	9/6/07 1:39 PM	8 KB
	22	Global Knowledge	Over 50 New Courses from Global Knowledge	9/6/07 1:00 PM	8 KB

# Simple Administration

Sendio I.C.E. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://ibx.sendio.com/sendio/ice/ui/

Headlines News CNET GP MapQuest Maps AA Expedia Wikipedia NetSuite AdWords XO MyFax Sendio Sandbox ProjectPath Sendio IBX GoToWebinar Sendio ICE House

**Sendio I.C.E.** Logged in as Tim Lee-Thorp

User

Admin

System

Global Views

Directories

Domains

Accounts

Addresses

Logs

Logout

The System

Options Contacts Inbound Control Outbound Control SSL SilverList

Unassigned Attachment Policy  Allow

Address Validation

Unknown Recipient Address  Reject

Sender Domain Unregistered  Defer

Sender Domain Lookup Error  Defer

SilverListing

SilverListing  Enabled

SilverListing Error  Allow

Sender IP Address

Sender IP Address Bad Reputation  Allow

Sender IP Address Unknown  Allow

IP Reputation Service Outage  Allow

Anti-Virus

Virus Infected  Reject

Virus Suspected  Reject

Virus Unscannable  Allow

Anti-Virus Service Outage  Defer

Zero-Hour

Zero-Hour  Reject

Zero-Hour Service Outage  Allow

Bulk

Bulk Tagging Service Outage  Allow

DKIM

DKIM Signature Checking  Enabled

DKIM Signature Bad  Allow

DKIM Signature Lookup Error  Allow

DomainKeys

DomainKeys Signature Checking  Allow

Save Options Undo Changes

Copyright 2007 Sendio, Inc. 4.1.20070913.2-qa

Transferring data from ibx.sendio.com...

# Summary

- eMail, the most important business tool, is under siege
- The status quo to defend it, the spam filter, is a failure

The Sendio I.C.E. Box provides email integrity

You need to trust your business communications...

**SAVE  
SPAM MAIL**



**Sendio, Inc.**  
1176 Main Street, Suite C  
Irvine, CA 92614

949.274.4375 tel  
info@sendio.com

[www.sendio.com](http://www.sendio.com)