



# **I Know Spam When I See It**

**Windows Technical Forum**

**February 3, 2003**

Dave Strickler, CEO  
[www.mailwise.com](http://www.mailwise.com)

# What you'll get out of this session:

- **A better understanding of Spam**
  - What it is, and how much is out there
- **Technical Tips you need to minimize Spam**
  - Tricks the Spammers use, and how to combat them
- **Executive briefing on products to help you run a clean E-mail system**
  - What kinds of products are out there
- **A demo on MailWise after the presentation**

# Who is MailWise and DWS ?

- **Founded in 1985 (17 years old)**
- **100% dedicated to E-mail solutions**
- **Currently managing over 500,000 mailboxes**
- **Customers include:**



# “Spam”

What is it, and how  
much is out there?

# What is Spam ?

- **All Spam is Unsolicited Commercial E-mail**
  - You didn't ask for it
  - It's selling something (Porn, Credit cards, Scams)
  - But if you want it, is it Spam ?
- **We all get Spam in the US Postal Mail**
  - It's regulated by Federal Law
  - It uses your tax dollars to arrive in your mailbox
- **... and we get Spam in our electronic mail**
  - No one wants to regulate it (although States are trying)
    - Would you want to be labeled Anti-Business ?
  - It uses your Internet connection, wastes employee time, etc.

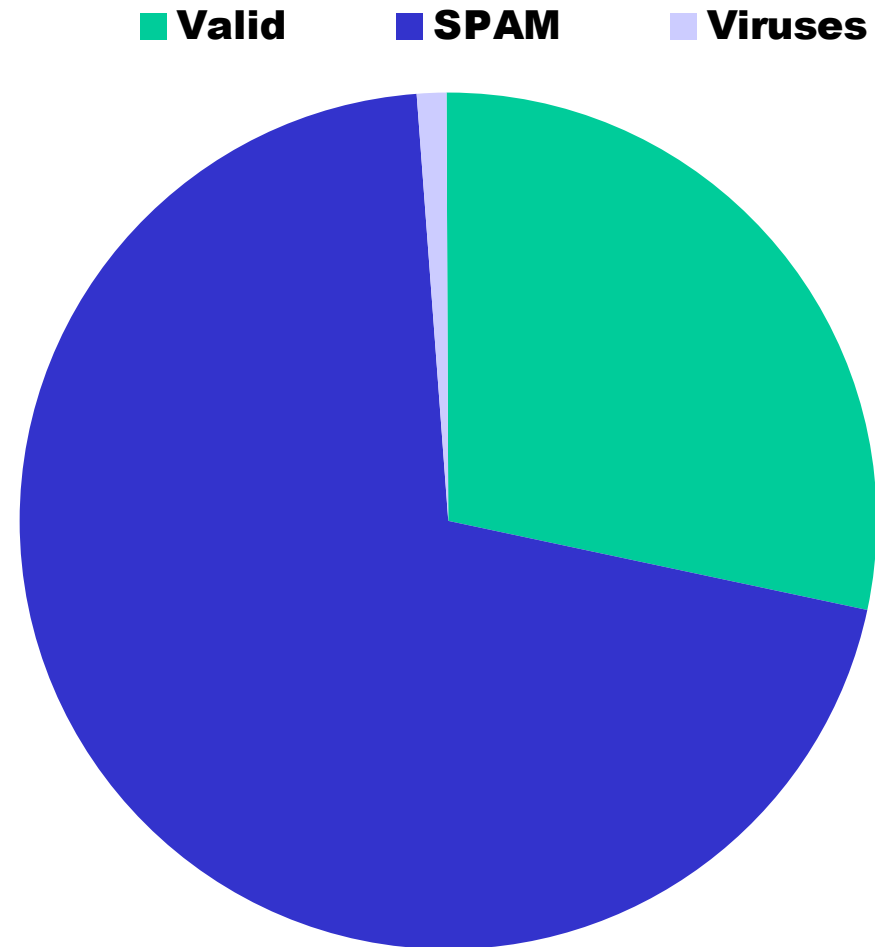
# How much Spam is out there ?

- **Ferris Research**

- \$10 Billion in costs to US Businesses in 2003

- **MailWise**

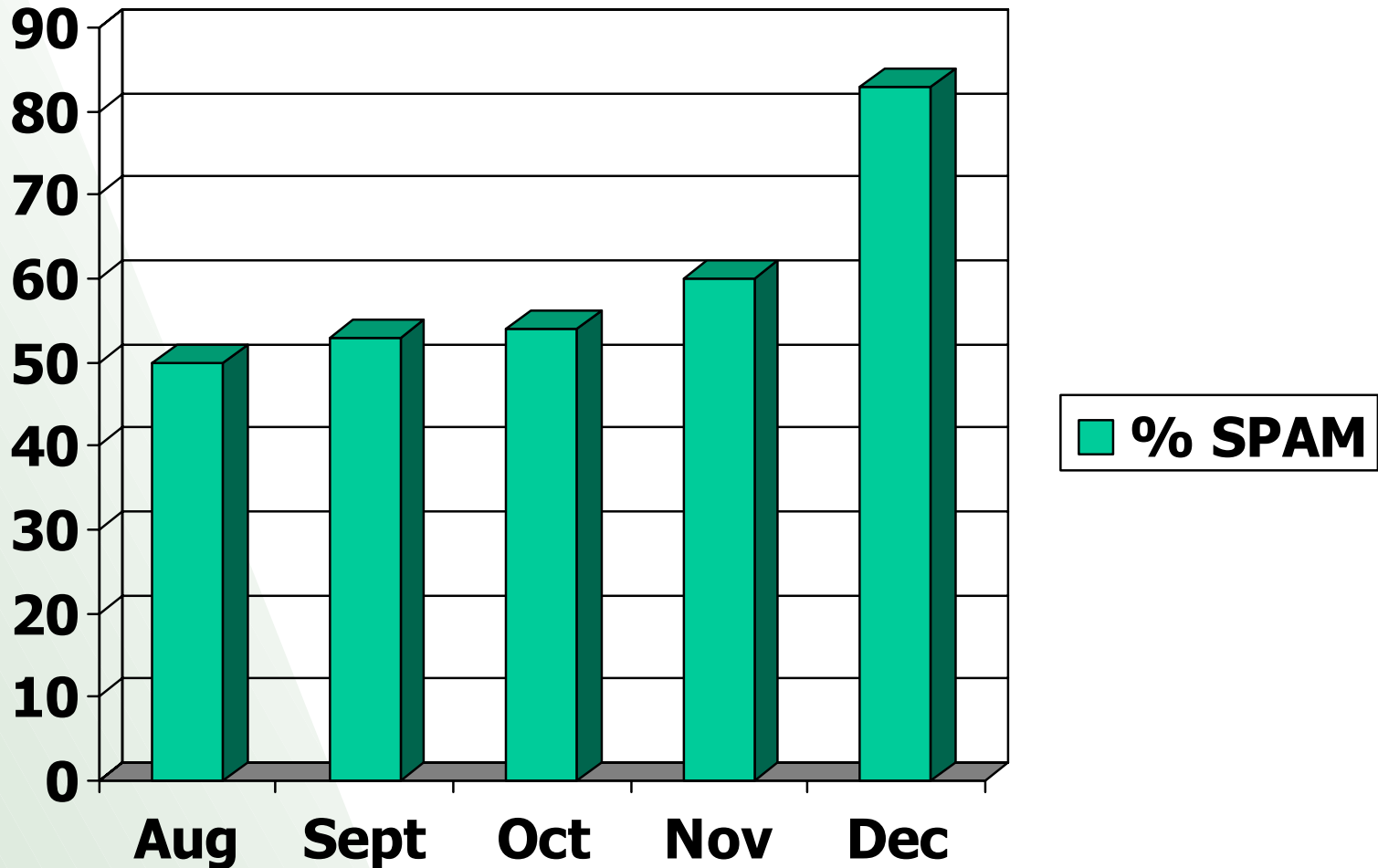
- 60% - 80%



## Quick Spam Stats for the U.S.

- **2.9 Billion Spam messages each month**
- **18.8 Terabytes of Spam each month**
- **Cost to U.S. businesses each month:  
\$660 Million**

# ... and the problem is getting worse



# Problems Caused by Spam

- **Spam comprises 60%-80% of all E-mail**
  - Anyone reporting lower stats means they aren't catching it all
- **Results of allowing Spam:**
  - 60% - 80% increase in Internet pipe load
  - 60% - 80% more load on your SMTP server
  - 60% - 80% more storage space needed
  - 60% - 80% larger databases = more corruption
  - 60% - 80% slower maintenance routines
  - 60% - 80% more backup media required
  - 60% - 80% slower backups & restores
  - ... All this increases your workload !

# More problems from Spam

- **Legal and H.R. issues with offensive E-mails arriving in employee mailboxes**
- **Wasted employee time having to wade through 60%-80% of their new mail**
- **Opening Spam often leads to viruses & other malicious code being executed**
- **Unsubscribing *guarantees* that more Spam will arrive**

# How can you detect Spam ?

# Detecting Spam

- **Rudimentary methods: RBL & Keyword**
  - Checking "FROM:" e.g. *freestuff@yahoo.com*
    - Spammers never use the same address twice
    - RBLs (Realtime Black Lists) are only a slightly better method (10%-15% effective) and create false-positives (5%-10%)
    - Have you ever been listed on on by mistake?
  - Finding keywords: e.g. "breast" in the subject
    - Too many false-positive hits
    - Who maintains the ever growing list of keywords?

# Detecting Spam

- **Automated methods:**
  - Look in the Header
    - Malformed headers indicate sloppy code which Spammers are known to use
  - “Read” the E-mail like a human does
    - Use a A.I. approach to understanding E-mail
  - Remember: Don’t accept inferior results !
    - Trap 99% of your Spam or else...
    - Would you buy a virus checker that only caught 50% of your viruses ?

## Method Details: Header Info

Received: from mail.dcemail.com  
([200.30.77.68])  
by mail.yahoo.com; Tue, 24 Sep 2002 02:10:40 -0400  
X-MSMail-Priority: Normal  
Message-Id: LASUV57EV.leonsykes @sacbeemail.com  
Content-Type: text/html; charset="us-ascii"  
Return-Path: danapoint@mypersonalemail.com  
From: leonsykes@sacbeemail.com  
Received: from mail.dcemail.com by 21B60E5.mail.dcemail.com with  
SMTP for Joe@yahoo.com; Tue, 24 Sep 2002 06:56:18 -0400  
Date: Tue, 24 Sep 2002 06:56:18 -1800  
To: Joe@yahoo.com  
Reply-To: danapoint@fresnomail.com  
Subject: Advertise to Millions via the Internet  
Content-Transfer-Encoding: 7bit  
X-Mailer: Internet Mail Service (5.5.2650.21)

# Header Info: From Who?

Received: from mail.dcemail.com  
([200.30.77.68])  
by mail.yahoo.com; Tue, 24 Sep 2002 02:10:40 -0400  
X-MSMail-Priority: Normal  
Message-Id: LASUV57EV.leonsykes @sacbeemail.com  
Content-Type: text/html; charset="us-ascii"  
Return-Path: [danapoint@mypersonalemail.com](mailto:danapoint@mypersonalemail.com)  
From: [leonsykes@sacbeemail.com](mailto:leonsykes@sacbeemail.com)  
Received: from mail.dcemail.com by 21B60E5.mail.dcemail.com with  
SMTP for Joe@yahoo.com; Tue, 24 Sep 2002 06:56:18 -0400  
Date: Tue, 24 Sep 2002 06:56:18 -1800  
To: Joe@yahoo.com  
Reply-To: [danapoint@fresnomail.com](mailto:danapoint@fresnomail.com)  
Subject: Advertise to Millions via the Internet  
Content-Transfer-Encoding: 7bit  
X-Mailer: Internet Mail Service (5.5.2650.21)

# Header Info: Strange Times and Zones

Received: from mail.dcemail.com  
([200.30.77.68])  
by mail.yahoo.com; Tue, 24 Sep 2002 **02:10:40** -0400  
X-MSMail-Priority: Normal  
Message-Id: LASUV57EV.leonsykes @sacbeemail.com  
Content-Type: text/html; charset="us-ascii"  
Return-Path: danapoint@mypersonalemail.com  
From: leonsykes@sacbeemail.com  
Received: from mail.dcemail.com by 21B60E5.mail.dcemail.com with  
SMTP for Joe@yahoo.com; Tue, 24 Sep 2002 **06:56:18** -0400  
Date: Tue, 24 Sep 2002 06:56:18 **-1800**  
To: Joe@yahoo.com  
Reply-To: danapoint@fresnomail.com  
Subject: Advertise to Millions via the Internet  
Content-Transfer-Encoding: 7bit  
X-Mailer: Internet Mail Service (5.5.2650.21)

# Would your Spam catcher trap this ?

Dear Friend,

I want to tell you that I have F\*R\*E\*E V\*I\*A\*G\*R\*A and other things that I'm sure you're interested in. Call me at 877-222-1234 for a packet. Or visit our web site at <http://129.23.122.13/sample>

# Only very clever software would see:

Dear **Friend**,

I want to tell you that I have **F\*R\*E\*E V\*I\*A\*G\*R\*A** and other things that I'm sure you're interested in. Call me at **877-222-1234** for a packet. Or visit our web site at <http://129.23.122.13/sample>

# Fighting the Battle On Your Own

- **Stop known IPs at your network firewall**
  - This will block both good and bad E-mail from an IP
  - Difficult to keep a “list” of IPs
- **Block E-mail addresses on your SMTP**
  - Difficult to keep a “list” of addresses
  - Updates must be done *by hand*
- **Block on the desktop with Rules**
  - Maintained at the user/desktop level
  - High probability of error

# What you can put in place to stop Spam

# Anti-Spam Solutions Overview

- **Desktop / Server - Appliance / ASP**
- **Check for features**
  - How much work do I have to do ?
  - Basic filtering technology: simple or robust ?
  - How configurable: down to the user level ?
  - How do updates to filters work ?
    - Cost ?
    - Who installs them ?
    - Who tests them and insures they work ?

# Understanding Anti-Spam software

- **Desktop**
  - Made for personal use
  - Typically for Win32/Outlook only
  - Gets end-user involved in Rule maintenance

# Understanding Anti-Spam software

- **Server or Firewall**
  - Made for medium to large businesses
  - Proprietary to the Server / Firewall
  - Expensive installation
  - Requires maintenance effort by the E-mail Admin

# Understanding Anti-Spam software

- **Appliance**
  - Made for large businesses
  - Expensive initial cost
  - Requires maintenance effort by the E-mail Admin
  - Proprietary hardware – what if it breaks?

# Understanding Anti-Spam software

- **ASP**
  - Made for businesses of all sizes
  - Instant “installation” and payback
  - Billed monthly - *no Capital costs*
  - Requires no extra effort from E-mail Admin
  - Acts as a “Plan B” for E-mail backup

# MailWise Filter – [www.mailwise.com](http://www.mailwise.com)

- **ASP based**
  - No hardware or software to buy, install or upgrade
- **Traps 99.7% of Spam**
  - Uses over 6,500 heuristic rules for detecting Spam
- **Gartner: Thumbs-Up**
  - Featured in Gartner Group's January 2003 report, "Anti-Spam Products for Enterprises".
- **Free 21-day free trial**
  - We know it works – try it for 3 weeks for free and watch your Spam disappear.

## Wrap-Up

- **Putting an Anti-Spam solution in place saves employee time and your company's money**
  - [www.mailwise.com/roi](http://www.mailwise.com/roi)
- **Demand at least 99% of Spam get caught by any software**
- **Contact Information**
  - [www.mailwise.com](http://www.mailwise.com) or (800) 999-5412
  - [dstrickler@mailwise.com](mailto:dstrickler@mailwise.com)