How UO Deals With Spam: A Brief Strategic Overview With Some Tactical Suggestions

Cornell/Educause Institute for
Computer Policy and Law
July 8th, 2004

Joe St Sauver, Ph.D. (joe@uoregon.edu)
University of Oregon Computing Center

http://darkwing.uoregon.edu/~joe/icplspam/

My Charge from Steve:

- Steve Worona asked me to:

  … do a "case study" on Oregon's SPAM-control system, including how it works technically, what the users see, how you devised it, how people like it, what other options you considered, etc.

  We'll see what we can get through in our twenty minute slot, trying to keep it at a reasonable level of geekyness. :-)

The Obligatory "One Slide" Executive Summary

- While many universities filter spam using content based filtering tools such as Spam Assassin, we filter spam based on **where mail comes from using blacklists and local filters:**
  -- we reject mail from known spammers
  -- we reject mail from insecure hosts
  -- we reject mail from ISPs that consistently ignore abusive users, and
  -- we make mail from dialup/DSL/cable modem users go via the ISP's mail server
- **==> Our users get virtually no spam.**

I. Email The Way It Used to Be

Life, without spam.

The UO End User Email Experience

- Our goal (and what our users usually see): little if any spam on our large central systems.
- Most users see <u>none</u> (zero spam per day). Some users will occasionally see "whack-a-mole" spam pop up from a reputable provider who briefly has a bad customer.
- True anecdote: every once in a while we get complaints about spam getting "bad:"
  "Hey, what is <u>going on</u> over there!
  I got <u>three</u> spam in my mail this last week!!!"

When Spam Does Slip Through…

- When spam does slip through our default local filters, we ask UO faculty, students and staff to send us a copy so we can report it to the responsible provider (we like http://www.spamcop.net for this). We also use those reports to tweak our local filters.
- We routinely report spamvertised domains with bad whois data to wdprs.internic.net – those domains then get fixed or disabled.
- It is key that users provide us with <u>timely</u> and <u>usable</u> reports…

Our User Spam Reporting Expectations

- Our goal is to get users to the point where they can consistently:
  -- report only spam they receive (not viruses, not legitimate message traffic), which was
  -- sent directly to one of our spam-filtered systems (not sent through some off site mailing list, departmental hosts, Hotmail, etc.),
  -- to the right local reporting address, within
  -- a day or so of the time the spam was sent,
  -- forwarded with **full/expanded headers** (and with the rest of the message body there, too).

Spam Arriving Via Offsite Mailing Lists

- Occasionally users see spam that came in via some mailing list they're on that's hosted elsewhere. Assuming you use the approach outlined in this talk, spam needs to get filtered by the site that first receives the spam; once the spam has hit a mailing list, it’s too late for us to do anything about it. Users need to get the site that's hosting the list to fix their filtering, convince the list owner to make her list closed/moderated, quit the list, live with the spam, or do content based filtering.

Users Need to Forward Spam, Not Use "Bounce"

- Users also need to know that they must use the forward command to report spam they receive (rather than "bouncing" it).
- Why? Forward preserves the integrity of the Received: headers, while the bounce command commingles the original headers with the headers of the person bouncing the message to you, making it hard to process and report that spam appropriately.

Full Headers...

- Anyone who works on abuse handling/spam management will tell you that the biggest obstacle to users effectively reporting spam they're getting is teaching them to enable full headers. Full headers are <u>absolutely essential</u> to a filtering regimen that relies on "where mail comes from," as ours does.
- Oregon has built a nice set of how-to-enable full header pages; you're welcome to use them as the basis for your own how-to-enable full header pages. See http://micro.uoregon.edu/fullheaders/

The Importance Of Users Having Healthy Skepticism

- The other thing you need to inculcate in your users is a sense of healthy skepticism:
  -- No, you do not need to “verify” your Visa information or your eBay/PayPal password.
  -- No, there aren't millions of dollars waiting to be shared with you in Nigeria. Really.
  -- No, our staff would never ask you to email them your account password.
- Healthily skeptical users are robustly resistant to phishing and online scam spams.

II. The Mechanics of How We Filter

Blacklists

- **Like UO, your university can successfully block the vast majority of spam at connection time simply by using a few free (or cheap) DNS blacklists.**
- At the U of O, we use:
  -- the www.mail-abuse.com RBL+ blacklist,
  -- the www.spamhaus.org SBL+XBL, and
  -- the njabl.org NJABL DNSBL.
- If you use DNSBLs as we do, endeavor to run copies of those DNSBL zones locally.

Locally Maintained Filters As An Adjunct to Blacklists

- Even when using multiple blacklists, you may optionally want to supplement them with local filter rules. We’re relatively, uh, “enthusiastic,” augmenting the three DNSBLs we use with about 5,100 locally maintained domain- or CIDR- netblock-oriented rules. If you use sendmail as we do, you’ll implement these local filters via /etc/mail/access
- cidrexpand is your friend

DNSBLs Plus Local Filters Work Really Well

- Blocking takes place while the remote mail server is still attached; this means that we can reject unwanted SMTP connections and immediately return the reason to the connecting MTA; no problems with spoofing.
- Spammer content tweaking become irrelevant
- Blocking a single bad connection can translate to avoiding 10K+ pieces of spam; that sort of filtering scales extraordinarily well.

Miscellaneous Filters

- In addition to using DNSBLs augmented by local filters, we also use some miscellaneous filters such as:
  -- virus filters (beyond the scope of this talk)
  -- anti-SMTP-relay filters (which everyone uses these days)
  -- some SMTP Mail From: validation checks
  -- a few other miscellaneous rules
- The key components are the DNSBLs plus local filter rules.

Blocked SMTP Connection Attempts Per Day For Selected Days on Two UO Systems

Date	Gladstone	Darkwing	Total
Sun 14 Jul 2002:	7,405	1,606	9,011
Mon 14 Oct 2002:	16,794	3,452	20,246
Wed 14 Jan 2003:	18,562	5,813	24,375
Mon 14 Apr 2003:	18,714	4,925	23,639
Mon 14 Jul 2003:	15,998	5,116	21,114
Tue 14 Oct 2003:	119,393	9,786	129,179
Thu 15 Jan 2004:	33,289	13,479	46,768
Wed 14 Apr 2004:	59,845	28,339	88,184
Sat 15 May 2004:	59,376	25,401	84,777
Mon 14 Jun 2004:	45,005	49,998	95,003
Thu 24 Jun 2004:	66,550	58,735	125,285

Note #1: Gladstone is our student server, with 27K accounts; Darkwing is our faculty/staff server with 13.5K accounts

Note #2: These are blocked SMTP CONNECTIONS, not blocked MESSAGES. A single SMTP connection may represent 1, 10, 100 or 1000 (or more) MESSAGES.

Note #3: Blocked connections may include viral traffic as well as spam.

III. How Do You Decide Which Email Sources to Block?

Picking DNSBLs

- When you pick a DNSBL, you are effectively trusting someone else’s recommendations about what you should block. Not all DNSBLs are equally trustworthy (or efficacious). Research any DNSBL you consider before trusting it with institutional email filtering decisions.
- The three DNSBLs we currently use and recommend all have excellent reputations; they are conservative, accurate and effective.

Building Local Filter Rules

- Local filter rules are a different business.
- YOU need to decide what to block or not block, typically based on:
  -- characteristics of the spam samples you see
  -- user complaint volumes per domain or range
  -- the ISP’s response to complaints lodged with them
  -- the ISP’s reputation in general
  -- the likelihood that blocking the site will substantially interfere with legitimate mail

Spam Zombies==> 80% of Spam

- At least 80% of current spam is sent via spam zombies -- end user hosts (usually connected by cable modem or DSL) which have been compromised by viruses or other malware and turned into spam delivery appliances without the knowledge or permission of the system owner.
  (see: http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/ and http://www.sandvine.com/solutions/pdfs/spam_trojan_trend_analysis.pdf)

ASNs With 1% or More of 4 Million Open Proxies/Spam Zombies (7/3/04)

#1	AS4134	Chinanet Backbone, Beijing	201896	5.02%
#2	AS7132	SBC Internet Services, Plano Texas	169547	4.21%
#3	AS4766	Korea Telecom	144778	3.60%
#4	AS7738	Telecom. da Bahia, Brasil	139583	3.47%
#5	AS1668	AOL Transit Data Network	125320	3.12%
#6	AS9318	Hanaro Telecom, Seoul Korea	117645	2.92%
#7	AS3320	Deutsche Telekom	111052	2.76%
#8	AS8151	Uninet, Mexico	103494	2.57%
#9	AS27699	Telecom. de Sao Paulo, Brasil	91430	2.27%
#10	AS3215	France Telecom Transpac	87617	2.18%
#11	AS8167	Telecom. de Santa Catarina, Brasil	82499	2.05%
#12	AS4812	China Telecom, Shanghai	71702	1.78%
#13	AS4837	CNCGroup/China169 Backbone	65767	1.63%
#14	AS9277	Thrunet, Seoul Korea	56378	1.40%
#15	AS3462	Hinet/Chungwha Telecom, Taiwan	52469	1.30%
#16	AS4813	China Telecom, Guangdong	43236	1.07%
			Total:	41.35%

See http://darkwing.uoregon.edu/~joe/jt-proxies/ (PDF or PPT format)
http://darkwing.uoregon.edu/~joe/one-pager-asn.pdf

Spam From Just One Broadband Provider

- "Comcast users send out about 800 million messages a day [e.g., ~292 billion/year], but a mere 100 million flow through the company's official servers. **Almost all of the remaining 700 million [messages] represent spam**…" (http://news.com.com/2010-1034-5218178.html) (May 24, 2004)
- "On Monday [June 7, 2004], the company began targeting certain computers on its network of 5.7 million subscribers that appeared to be sending out large volumes of unsolicited e-mail. Spokeswoman Jeanne Russo said that in those cases, it is blocking what is known as port 25, a gateway used by computers to send e-mail to the Internet. The result, she said, was a 20 percent reduction in spam." http://www.washingtonpost.com/wp-dyn/articles/A35541-2004Jun11.html

Responsible ISPs Controlling Direct-to-MX Spam By Filtering Port 25

- As mentioned in the Comcast article, some responsible ISPs (and some universities) keep direct-to-MX spam (typically from open proxies or spam zombies) from leaving their networks by filtering port 25 (SMTP) traffic, allowing mail to be sent only via their official mail servers.
- Legitimate mail **can still be sent**, those messages just need to be sent via the official SMTP server the provider maintains.

Examples of Schools That Have Filtered Port 25, Either Campus-Wide or For a Subset of Users (or Have Plans to Do So)

- **Buffalo**: http://cit-helpdesk.buffalo.edu/services/faq/email.shtml#2.2.6
- **CWRU**: http://tiswww.case.edu/net/security/smtp-policy.html
- **MIT**: http://web.mit.edu/ist/topics/email/smtpauth/matrix.html
- **Oregon State**: http://oregonstate.edu/net/outages/index.php?action=view_single&outage_id=214
- **TAMU**: http://www.tamu.edu/network-services/smtp-relay/
- **University of Florida**: http://net-services.ufl.edu/security/public/email-std.shtml
- **University of Maryland Baltimore County**: http://www.umbc.edu/oit/resnet/faq.html#smtp-current-policy
- **University of Missouri**: http://iatservices.missouri.edu/security/road-map.html#port-25 (as of June 30, 2004)
- **WPI**: http://www.wpi.edu/Admin/IT/News/networkingnews.html#newsitem1059685336,32099,

Sometimes Providers Offer DNS “Hints” So You Can Filter Mail “For Them”…

- Many cable modem and DSL providers have begun to use distinctive domain naming for their cable modem and DSL customers (such as addresses with a pattern such as: <foo>.dsl.telesp.net.br).
- Having identified addresses of that sort, it is easy to block traffic coming directly from those hosts even if the provider doesn’t filter customer port 25 traffic themselves.

That “Hinting” is Becoming Common in the Commercial ISP Space…

*.adsl-dhcp.tele.dk

*.cable.mindspring.com

*.client.comcast.net

*.customer.centurytel.net

*.dial.proxad.net

*.dsl.att.net

*.dynamic.covad.net

*.ppp.tpnet.pl

- Consistent naming would be nice (but isn’t likely)

A Gotcha Some DSL Users May Run Into:

- 1) They register a vanity domain and point that domain at their DSL connection, BUT
  2) They fail to create a corresponding PTR (reverse DNS number-to-name) record, and
  3) They fail to route their outbound email through their provider's SMTP server.
- These guys get blocked when their server’s address resolves to <foo>.dsl.<bar>.com rather than the vanity domain.
- They need to fix their reverse DNS or they need to use their provider’s SMTP server

Another Option: Sender Policy Framework

- SPF allows mail servers to identify and block forged envelope senders (forged “Return-path addresses”) early in the SMTP dialog by doing a simple DNS-based check of a site’s text record.
- *Many* major providers and clueful sites are now publishing SPF records, including AOL (~24.7M subscribers), Columbia, Delaware, Google, GNU.org, Iowa State, Oreilly.com, Oxford.ac.uk, Outblaze (>30M accounts), perl.org, SAP.com, South Carolina, spamhaus.org, w3.org, symantec.com, UCSD, etc.
- What about your college or university?

```
% host -t txt example.edu
```

SPF Implementation Issues

- Adoption of SPF can be done “asymmetrically” – you can publish your own SPF record but not query others, or vice versa.
- If you’re used to doing email forwarding, get used to doing email rewriting (see the FAQ cited below)
- Roaming users <u>will</u> develop a sudden interest in VPNs and/or authenticated remote access
- The FTC has recognized the importance of domain level authentication systems such as SPF; see p.12 of http://www.ftc.gov/reports/dnsregistry/report.pdf
- Want more information? http://spf.pobox.com/ (the FAQ there is particularly helpful)

Making Decisions About the Rest of It

- In the "old days," the Internet worked because most people on the net weren't jerks. If a local jerk did pop up, they were educated or kicked off. You took care of yours; other folks took care of theirs. **Your site valued its reputation**.
- **Times changed**. RBOCs got involved in offering Internet service. Large ISPs came online overseas. Struggling backbones took whatever customers they could get. Malware began to compromise 100s of 1000s of hosts. **The neighborhood went to hell**.

Trust Responsible Sites

- Today there are **still** sites, in fact **MOST** sites, which work very hard to deal with security issues (and that includes most of higher education).
- Responsible sites take compromised hosts offline as soon as they're detected. They accept and investigate abuse reports. They refuse to allow spammers to use their facilities.
- Mail from those sites will seldom be a problem.
- They're "good neighbors." Accept mail from them. If something goes wrong and you see spam from them, let them know. They'll take care of it.

Shun Sites Which Tolerate Abuse

- Other sites, however, don’t really much care if their customers are infested, or if they’re providing connectivity to spammers.
- These irresponsible sites ignore abuse reports (or are overwhelmed by the volume of abuse reports they see), and network abuse incidents never gets resolved.
- These sites could address their problems, just as the responsible sites do, but **they choose not to do so**. They’re relying on others tolerating their abuse.
- You’ll get lots of spam from those sort of sites.
- They’re “bad neighbors,” and they’ll ruin mail for your users, if you let them. Decline to accept mail from them until they take care of their problems.

Data Points: Reputation Databases

- http://www.senderbase.org/ provides email volume estimates for domains and top sending IP addresses. Some of the names you'll recognize, some you won't.
- http://www.mynetwatchman.com/ provides information about activity seen by its distributed network of sensors, as does SAN's Internet Storm Center Source Report (http://isc.sans.org/source_report.php)
- http://www.openrbl.org/
- http://www.spamcop.net/

A Data Point: Spamhaus.org’ Top 10 Worst Spam ISPs May 2004

- #1 **MCI** (US): 186 entries (with 45 ROKSO entries[*])
  #2 **Savvis** (US): 118 entries (35 ROKSOs)
  #3 **Kornet.net**: 123 entries (2 ROKSOs)
  #4 **Above.net** (US): 94 entries (16 ROKSOs)
  #5 **Chinanet-CQ**: 106 entries (55 ROKSOs)
  #6 **Chinanet-GD**: 103 entries (41 ROKSOs)
  #7 **Comcast** (US): 81 entries (5 ROKSOs)
  #8 **Level3** (US): 67 entries (21 ROKSOs)
  #9 **Interbusiness.it**: 73 entries (0 ROKSOs)
  #10 **Verizon.net** (US): 62 entries (9 ROKSOs)

-----

[*] ROKSO=Register of Known Spam Operations, hard line spam operations that have been terminated by a minimum of three consecutive service providers for serious spam offenses.

Another Data Point: Understanding the China Problem

- ‘Five countries are hosting the overwhelming majority - a staggering 99.68 per cent - of spammer websites, according to a study out yesterday [e.g., June 30th, 2004]

  ‘Most spam that arrives in email boxes contains a URL to a website within an email, to allow users to buy spamvertised products online. While 49 countries around the world are hosting spammer websites, unethical hosting firms overwhelmingly operate from just a few global hotspots. Anti-spam vendors Commtouch reckons 73.58 per cent of the websites referenced within spam sent last month were hosted in China, a 4.5 per cent decrease from May. South Korea (10.91 per cent), the United States (9.47 per cent), the Russian Federation (3.5 per cent) and Brazil (2.23 per cent) made up the remainder of the "Axis of Spam".’
  http://www.theregister.co.uk/2004/07/01/commtouch_spam_survey/

- China Anti-Spam Workshop Trip Report
  http://www.brandenburg.com/reports/200404-isc-trip-report.htm

IV. Achieving the Balance

“You’re Filtering Us!”

- Occasionally (maybe a couple of times a month), someone who’s blocked contacts us to complain or to inquire about why they’re blocked. In that case, we talk about what we’re seeing and we’re often able to resolve the underlying problem and unblock that site.
- We use sendmail’s defer_checks to make sure that we can accept “we’re blocked?” inquiries on RFC2142 operational contact addresses.
- Most ISPs simply silently accept the fact that they’re blocked (they <u>really</u> don’t care).

“You’re Filtering Something I Really Want/Need to Get!”

- If we end up filtering mail that a local user *really* wants to get (e.g., mail from a family member; a subscription newsletter), the user can opt out of our default spam filtering via a web page that creates a “.spamme” file in their home directory; a system cron job looks for those files hourly and then exempts those users from filtering. (That same page can be used to re-enable filtering, too.) See: cc.uoregon.edu/cnews/winter2004/optout.html

Given the Chance, Do People Opt Out of Default Filtering?

- If you do a good job of filtering, requests to opt out of default system-wide filtering will be rare.
- As of 7/3/04 here at UO….
  -- 13 of 27329 UO student accounts have opted out of our default spam filtering (0.04% opt out rate)
  -- 84 of 13587 faculty/staff accounts (including role accounts, email aliases and mailing lists) have opted out (0.61% opt out rate)

Given Those Sort of Numbers, Spam Filtering Is (and Should Be) Enabled By Default

- Assume that 99% of all users are irritated by spam, want it to go away, and will either welcome spam filtering or be ambivalent about its presence.
- If you have 20,000 users, that implies you can either make 19,800 users “opt-in” to optional filtering or you can make 200 users “opt-out” of default filtering. (So why do so many sites make spam filtering optional?)

Since This Isn’t Lunchtime, An Analogy to Drive Home the Point

- *Assume you’re running a restaurant that has a fly-in-the-soup problem.*

  You can make thousands of customer ask to have the flies in their soup removed, or you can have the one guy in a million who LIKES flies in soup ask to have the flies left in. Which makes the most sense?

There Are Some Accounts Which MUST NOT Be Filtered By Default

- While the default recommendation is, and should be, that accounts get spam filtered by default, there are some accounts which by their very nature MUST NOT be filtered by default. Those accounts include RFC 2142-mandated abuse reporting addresses such as abuse@, postmaster@, etc.
- Check to see if your site is listed on http://www.rfc-ignorant.org/
- There are other exceptions, too…

For Example: Admissions Inquiry Accounts

- For example, if we block some "spam" directed at our admissions office, might our admissions folks miss requests for information from potential enrollees? What's the net cost to the institution if we lose tuition revenue from ten (or a hundred) potential out of state students because we're blocking their inquiry email? [Estimated UO non-resident full time tuition and fees, 2003-2004, run $16,416 per academic year.]

Also Be Particularly Careful With Campus M.D.'s, Lawyers, etc.

- Under the Federal ECF (https://ecf.dcd.uscourts.gov/) email may now be used to transmit notices of legal pleadings. If email of that sort is sent to a University attorney and fails to get through, a default judgement may get entered when he/she misses a scheduled hearing.
- Or consider the patient of a teaching hospital surgeon who is unable to email her doc about her "chest pains," and then dies.

V. SpamAssassin

“Why Don’t You Just Use SpamAssassin?”

- We offer SpamAssassin as a user electable option, but SpamAssassin (or any content based filter) is not our default solution, and not necessarily a solution that we’d recommend (even though we do know that many of you use SpamAssassin or similar content based filters; see the separate spam filtering survey summary). Having said that, we’ll be the first to admit that content based filtering does have some good points.

One Obvious Point In Favor Of Content Based Filtering...

- One obvious point in favor of CBF is that there *is* some spam which is relatively constant, is readily detectable, and is trivially filterable based on its content.
- If you DON'T do CBF and easily identified spam ends up getting delivered, folks will ask, "How come the computer can't ID obvious spam messages when **I** can easily do so?" This is a (sort of) legitimate complaint.

Another Advantage Of CBF

- A second advantage of doing content based filtering is that it allows you to selectively accept some content from a given traffic source, while rejecting other content from that same source. This can be useful if you're dealing with a large provider (such as a mailing list hosting company) that has both legitimate and spammy customers, and you want to dump the spam but accept the legitimate traffic. (But wouldn’t it be better if the large provider kicked off their spammers?)

CBF Issues: False Positives

- On the other hand, one of the biggest issue with CBF is the problem of false positives. Because CBF uses a series of rubrics, or "rules of thumb," it is possible for those rubrics to be falsely triggered by content that "looks like" spam to the filtering rules but which actually isn't spam. For example, some (relatively crude) content based filters make it impossible for a correspondent to include certain keywords in a legitimate email message.

Using Scoring to Minimize False Positives

- Most content-based-filtering software, however, does "scoring" rather than just using a single criteria to identify spam. For example, a message in ALL CAPS might gets 0.5 points; if it also mentions millions of dollars and Nigeria, it might gets another 1.2 points; etc. Messages with a total score that exceeds a specified threshold get tagged as spam; the mere presence of a single bad keyword alone typically wouldn't be enough.

Picking a Spam Threshold

- A CBF issue that's commonly ignored by non-technical folks is choice of threshold value for spam scoring. The threshold value you pick will have a <u>dramatic</u> effect on the number of false positives you see, as well as the number of unfiltered spam you see.
- If you use SpamAssassin, what's your default threshold? 3? 5? 8? 20?
- Do you know the scoring rules you're using, and the weights those rules carry?

CBF And Privacy

- Doing content based filtering also implicitly seems "more intrusive" to users than doing non-CBF.
- Even when CBF is done in a fully automated way, users may still be "creeped out" at the thought that their email is being "scanned" for keywords/spam patterns, etc.
- "Big Brother" is a powerful totem, whose invocation should be avoided at all costs.

CBF Issues: The Arms Race

- Because CBF attempts to exploit anomalous patterns present in the body of spam messages, there's a continuous “arms race” between those looking for patterns, and those attempting to avoid filtering. (And remember, spammers can trivially “test drive” contemplated messages through their own copy of SpamAssassin to spot any problems that may block delivery)
- This process of chasing spam patterns and maintaining odd anti-spam heuristic rulesets is rather ad hoc and not particularly elegant.

Spammers Can Simply Out-and-Out Beat SpamAssassin

- I have no desire to provide a cookbook which will help spammers beat filters, so I won’t elaborate on this point except to mention one trivially obvious example: because Spam Assassin processing slows down as message size increases, SpamAssassin is generally configured to avoid scanning messages larger than a specific (locally configurable) size. If spammers send messages larger than that size, the spam will blow right past SA…

CBF and Scaling Properties

- As normally used, sites running Spam Assassin accept all mail addressed to their users, merely running the messages through SpamAssassin to score and tag them, perhaps (at most) selectively filing messages into a "likely spam" folder based on that scoring. Because of this, even if spam does get <u>eventually</u> discarded, you still need to install servers and networks able to initially absorb and temporarily store a virtually unbounded flow of spam. That doesn't scale well.

Indiana University's Specific Case…

- "When Indiana University installed its new e-mail system in 2000, it spent $1.2 million on a network of nine computers to process mail for 115,000 students, faculty members and researchers at its main campus here and at satellite facilities throughout the state. It had expected the system to last at least through 2004, but the volume of mail is growing so fast, the university will need to buy more computers this year [2003] instead, at a cost of $300,000. "**Why? Mainly, the rising volume of spam, which accounts for nearly 45 percent of the three million e-mail messages the university receives each day**."

  "The High, Really High or Incredibly High Cost of Spam"
  Saul Hansell, NY Times, July 29, 2003
  http://www.lexisone.com/balancing/articles/n080003d.html

Some Industry Spam %-age Estimates

- “Spam remained steady at 78% during May 2004.” (http://www.postini.com/press/pr/pr060704.html)

- ‘A report released last month by MessageLabs, Inc., an email management and security company based in New York, showed that nine out of 10 emails in the U.S. are now spam. Globally, 76 percent of all emails are spam. And Osterman [founder and president of Osterman Research] says the problem is only going to get worse. "In the next year to a year and a half, spam will account for 98 percent of all email," he says. "That's being pessimistic some would say. The optimistic forecast is that it will only get to 95 percent.”’ (July 1st, 2004) (http://www.internetnews.com/stats/article.php/3376331)

VI. Conclusion

A Note To Technical Folks Who May End Up Reading This Presentation

- Technical folks: whatever you decide to do about spam, be sure to talk to your university's attorney and your senior administrators before you implement any spam filtering strategy. Spam tends to be highly newsworthy, and there's a distinct chance you'll have a "Chronicle of Higher Education" moment if things go awry. Do NOT surprise your staff attorneys or your Chancellor/President/Provost.

In Conclusion: UO’s Really A Very Typical University

- UO’s really a very typical liberal arts state university of about 20,000 students.
- We face the same staff, financial and technical constraints that you face.
- We have a normal research university’s academic faculty (with normal research university faculty expectations)
- SO… if we can do something locally about spam, so can YOU!

Questions?

- Thanks for the chance to talk today!
- Are there any questions?