Higher Education Users and Spam: What Do Users Do When Things Go Wrong? How Have User Behaviors Changed Because of Spam?

Some Introductory Comments for a MAAWG Panel
MAAWG 9th General Meeting, San Francisco CA
January 29th-31st, 2007

Joe St Sauver, Ph.D. (joe@uoregon.edu)
MAAWG Senior Technical Advisor
http://www.uoregon.edu/~joe/behaviors/

Disclaimer: All opinions expressed in this document are solely those author and should not be taken as representing those of any other entity.

Higher Ed: A Diverse Environment With Many Different Types of Users

- The higher education email ecosystem has **many different types of users**: undergraduate and graduate students, their parents and families, teaching faculty, researchers, international collaborators, staff members, administrators, alumni, donors, institutional email senders, majordomo/listserv mailing list administrators, vendors, centralized and decentralized support staff.
- Moreover, there are wide differences in HOW email is deployed and used in higher education, with sometimes radically **different choices of technology, different usage policies, different filtering approaches**, etc.
- All of those factors affect how higher education-related users interact with their email, including unwanted email.

Given That…

- It would be presumptuous of me to pretend that I (or anyone!) could perfectly describe all the different issues that high education users run into when dealing with their email…
- The best I can do is to share **some** perspectives, and remind you that there are undoubtedly **many** others which are equally valid.
- Let's begin by considering a few of the ways that things can go wrong in conjunction with spam or anti-spam measures.

When Things Go Wrong #1: Spam Makes It Through

- One thing that can go wrong with email in higher education is that spam can end up making it through to the user's inbox, our best efforts notwithstanding.
- Predictably, users are not happy when this occurs.
- What do higher ed users do in that situation? They:
  -- **Complain** to IT staff & to dept/institutional leadership
  -- Try **manually blocking** the spam with filters they may build which are focused on spoofed message header From entries, or bad Subject keywords
  -- **Tinker with** their "this is spam" **threshold scores** (assuming it is customizable by them) ["Why can't I set the filtering threshold to a negative number?"]
  -- Try adding **additional filtering** (such as enabling a spam filter built into in the email program they use)

When Things Go Wrong #2: Worries About Mail Potentially Being Blocked

- Sometimes users may not receive mail that they're expecting, and not knowing how to check/tell what's up with that, they may become concerned that the mail which they're anxiously awaiting might be getting blocked (whether it actually is or not).
- Non-technical users may assume that spam filtering is done based on things like user visible From and Subject headers (when in reality it is seldom that simple), and users can become frustrated when a ten second answer to "how do you filter spam?" or "where's the list of addresses you're blocking?" simply isn't possible due to the complexity involved. (Quick! Try to explain DNSBLs, SURBLs, content scoring, Bayesian filtering, greylisting, DCC scoring, and all the other approaches you may be using… oops! Time's up!)

Worries About Inbound Mail Being Blocked (Continued)

- Best bet? Let users opt out of any or all filters if they want to do so, using an alternative filtering approach which best meets their needs. This may be key for folks in roles where non-delivery may have material financial consequences (e.g., admissions inquiries, donor relations contact addresses, etc.). If you're doing your job right, only 1-2% will typically choose this option.
- Alternatively: Don't "block" or "reject" anything, deliver everything either to the normal inbox or to a spam folder (this tends to get tricky when dealing with potential viral content), also allowing users to whitelist key correspondents who might otherwise get blocklisted.
- Yet another alternative is to provide daily summaries of what's been blocked on a user-by-user basis.

When Things Go Wrong #3: Wanted Email Does End Up Getting Blocked

- Other times the problem is that wanted inbound email does end up being blocked, our best efforts notwithstanding.
- Predictably, users are not happy when this occurs.
- What do higher ed users do in that situation? They:
  -- **Complain** to IT staff & to dept/institutional leadership
  -- Try **manually whitelisting mail** with entries based on From addresses or perhaps mailing list tags
  -- **Tinker with** their "this is spam" **threshold scores** (assuming it is customizable by them) ["Why do I see so much spam when I set my threshold score to 50?"]
  -- Try disabling some default **filtering** which might otherwise be on by default
  -- Ask correspondent(s) to **send from a different account, to a different address, as password'ed zip file, etc**

When Things Go Wrong #4: Outbound Email Ends Up Blocked

- Occasionally a higher ed institution unintentionally ends up having its outbound email blocked to a major provider (such as AOL), perhaps due to:
  -- an infestation of spam zombies or an open relay,
  -- overly aggressive institutional email marketing efforts,
  -- users forwarding all email messages before any filtering takes place,
  -- or for any of a host of other reasons.
- Predictably, users are not happy when this occurs.
- What do higher ed users do in that situation? They:
  -- **Complain** to IT staff & to dept/institutional leadership
  -- May be surprised that anyone would block them
  -- Temporarily or permanently **substitute** other accounts
- IT staff? They hustling to respond/resolve the issue

When Things Go Wrong #5: Intraspam

- Other times an institution ends up "self-spamming" or subjecting its users to one form or another of what might be called "intraspam." Intraspam often takes the form of institutional mailing lists which everyone is required to be on to receive important notices, which is fine, until the definition of what's an "important notice" softens and access to the list expands seemingly without bound.
- Predictably, users are not happy when this occurs.
- What do higher ed users do in that situation? They:
  -- **Complain** to IT staff & to dept/institutional leadership
  -- Try to unsubscribe (but they usually won't be able to)
  -- Filter the mail (sometimes missing truly important stuff)
- A committee will often be formed to study the matter.

When Things Go Wrong #6: User "Can't Send" While Traveling

- Eliminating open relays also complicates mail sending by legitimate users when they're on the road – "I can retrieve my mail just fine, but I can only reply to people who have an institutional email address; everything else returns some weird 'relaying denied' message and doesn't go out. Help!"
- Predictably, users are not happy when this occurs.
- What do higher ed users do in that situation? They:
  -- Skip doing email for a bit (withdrawal quickly ensues)
  -- Use institutional web mail to send outbound messages
  -- Configure their email client to use an alternative SMTP server at the site they're visiting (rare)
  -- Configure their email client to do SMTP Auth (rare)
  -- Install and use the institutional VPN product (rare)
  -- **Complain** to IT staff & to dept/institutional leadership :-)

How Have Higher Ed User Behaviors Changed Because of Spam?

Users No Longer Treat Email As A Reliable Communication Mechanism

- Because of the risk that email message may not be delivered, or if does get delivered, an important message may be lost in drifts and waves of spam, users no longer treat email as if it were an assured delivery communication mechanism.
- If a message isn't acknowledged, it may end up rapidly being resent, or email may be routinely followed up with a phone call or IM, or users may use IM instead of email, or users may not bother using email at all (ever wonder why it seems like there's a growing number of face-to-face meetings at many organizations?)
- Of course, email never really WAS an assured delivery communication mechanism, so this "change" is not necessarily all bad…

Users No Longer Treat Email As A Secure Communication Mechanism

- All the anti-spam scanning and filtering, even though it is virtually always done mechanically, also makes at least some users wonder if email is "secure" against eavesdropping.
- Of course, technical folks know that unencrypted email is NOT, and never has been, a secure communication mechanism, so having this be understood by the regular users is not a bad thing, except that in some cases it causes those regular users to reach for their unencrypted wireless Internet VoIP phone as a "more secure alternative!" – sometimes I just don't know what to say….

Some Prominent Higher Ed Users No Longer Even Use Email (Really!)

- http://www-cs-staff.stanford.edu/~knuth/email.html

  "*I have been a happy man ever since January 1, 1990, when I no longer had an email address. I'd used email since about 1975, and it seems to me that 15 years of email is plenty for one lifetime.*

  Email is a wonderful thing for people whose role in life is to be on top of things. But not for me; my role is to be on the bottom of things. What I do takes long hours of studying and uninterruptible concentration. […]

  So if you want to write to me about any topic, please use good ol' snail mail and send a letter to […]"

Others Have Substituted IM for Email

- "Large and growing numbers of teens—today's and tomorrow's college students—are regular users of IM [instant messaging], both as a personal communication tool and, in some cases, for educational initiatives in high school. As IM matures into an accepted means of communication, and as ever-larger numbers of students arrive on campus as seasoned IM users, colleges and universities are adding IM to campus functions ranging from recruiting and admissions to teaching and support. Some institutional libraries have set up online reference desks with IM applications, and faculty have begun using the technology to facilitate virtual office hours. For many current and prospective students, IM is becoming the preferred mode of contact with recruiters and admissions staff, the registrar's office, and academic advisors." *7 things you should know about... Instant Messaging*, www.educause.edu/ir/library/pdf/ELI7008.pdf

"We Outsource All Our Mailings To Avoid 'Spamming' or Having Our Regular Institutional Mail Blocked"

- Given the ease with which a sender can accidentally end up sending unwanted email (particularly if a mailing list gets built from hard-to-read handwritten "I'm interested, please tell me more!" postcards, many institutions have elected to outsource their institutional mailings to mailing service bureaus.
- Why? They fear that if they mail from their own institutional address space or their own institutional domains, those IPs or domains may end up being branded as spammy, with adverse implications for the entire institution.

"We Can No Longer Accept HTML Email, Nor Any Attachments via Email…"

- These measures are typically due to malware, not spam, but users just lump it all together as stuff that's "happening to them" because of "unwanted email."
- "DOD bars use of HTML e-mail, Outlook Web Access," http://www.fcw.com/article97178-12-22-06-Web , December 22, 2006:

  Due to an increased network threat condition, the Defense Department is blocking all HTML-based e-mail messages […] The JTF-GNO mandated use of plain text e-mail because HTML messages pose a threat to DOD because HTML text can be infected with spyware and, in some cases, executable code that could enable intruders to gain access to DOD networks

"Spam Has Interfered With How I Forward My Mail"

- Because traditional "dot forward" style Unix mail forwarding forwards mail before it goes through filters, the forwarding mail server often gets "blamed" for spam that it is just dutifully forwarding as instructed.
- Many users have been forced to change how they forward mail from one provider to another as a result, or in some cases institutions have outlawed email forwarding to eliminate this issue.
- See the discussion at "The Impending End of Traditional .forward-style Forwarding" at http://www.campus-technology.com/news_article.asp?id=10313&typeid=153

There Are Also Many More "Tactical" Responses To Spam Which Are Seen, Too

Some higher ed users may try to…

-- **"ignore spam"** (trying to pretend it really isn't a problem)

-- **"hide"** by removing all public references to their email address in institutional directories, on web pages, etc. ("munging" is a less extreme version of this behavior)

-- **"dodge"** by periodically changing their email address (assuming the institution will allow them to do so)

-- **"substitute"** an email address obtained from another provider (e.g., use a Yahoo, Gmail, AOL account, etc.), or by compartmentalizing email across multiple accounts

-- **"mock"** spam and spammers by poking fun at it/them

-- **"attack"** by conducting a crude mail bombing against the apparent sender (who unfortunately usually has nothing to do with the spam)

-- **"lend a hand"** by reporting spam, studying spam, etc.

You Get The Idea…

- Bottom line, spam has had *profound* impacts on how we communicate in higher education.
- I may be going out on a limb here, but I think most folks in higher ed would *love* to have things return to the way they used to be in "the good old days." Unfortunately, I'm not sure that will ever be possible, at least not in my lifetime.
- We've all adapted, and not necessarily for the better…