Using E-mail Safely and Well

M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies, Norwich University

Table of Contents

1 CC + REPLY ALL = TROUBLE: CONTROL VISIBLE DISTRIBUTION LISTS IN E-MAIL

Recently a nice lady in the Human Resources department at my university sent out a note to a dozen people reminding us that we had not yet finished signing up for our new medical insurance coverage.

Unfortunately, she put all the e-mail addresses into the CC (carbon copy) line where they were visible to everyone in the list. Predictably, someone on the list composed a response to her, hit REPLY ALL and sent some mildly personal information about the state of her medical concerns to all the recipients on the original list, none of whom cared a whit about her problems.

Luckily, there wasn't much that was very private in that message, but it did prompt me to write to the head of Human Resources about the incident. Part of my message was as follows:

> Many people unthinkingly use the CC line for addresses to a distribution list.
>
> Many people unthinkingly use REPLY ALL for replies to every e-mail message.
>
> The combination can lead to embarrassing violations of confidentiality; when the Human Resources (HR) department staff use CC instead of BCC (the BLIND CARBON COPY function that conceals the distribution list), the REPLY ALL function can inadvertently violate privacy.
>
> In this case, there was no particularly sensitive material revealed, but a different case could easily violate HIPAA (Health Information Portability and Accountability Act) and the University's rules on employee confidentiality.
>
> I'm sure that once your colleagues understand the issue, they will learn not to use CC for distribution lists when the intention is to communicate with individuals; by default, all of us should use the BCC list unless we need to stimulate group discussion of an issue or it's important for the members of the group to know who received the message.

It's important that we not dismiss this issue as too easy or too obvious to bother with. "Against stupidity, the gods themselves contend in vain," wrote Friedrich von Schiller in his "Maid of Orleans" (Die Jungfrau von Orleans) in 1801. Nonetheless, the CC + REPLY ALL habit becomes a covert channel for release of confidential information for people who refuse to keep an address book and simply look up any old e-mail and REPLY ALL to it as a lazy way of sending a new message.

If you doubt the seriousness of the problem, I suggest you look through your own archives of e-mail and count how many obvious cases there are of e-mails with inappropriate subject lines and inappropriate distribution lists sitting in your received-folders. I think you will be dismayed by the results of your research.

2 BCC PREVENTS E-MAIL NUISANCES

The consensus in our profession – despite the dreadful lack of hard statistics – is that something like 2/3 of all the damage caused to our information systems is from insiders who are poorly trained, careless or malicious (for a detailed discussion of security statistics see http://tinyurl.com/b6zzh or http://tinyurl.com/96u2n) . For example, a study published in late 2005 reported that "Sixty-nine percent of 110 senior executives at Fortune 1,000 companies say they are 'very concerned' about insider network attacks or data theft, according to a study by Caymas Systems, a network security technology firm based in San Jose, Calif. And 25 percent say they are so concerned they can't sleep at night, Sanjay Uppal, a vice president at Caymas Systems, told eSecurityPlanet." < http://tinyurl.com/mmnuw >

A McAfee-sponsored survey in Europe showed that (in the words of the Department of Homeland Security

Daily Open Source Infrastructure Report < http://www.dhs.gov/iaipdailyreport >), "Workers across Europe are continuing to place their own companies at risk from information security attacks. This "threat from within" is undermining the investments organizations make to defend against security threats, according to a study by security firm McAfee. The survey, conducted by ICM Research, produced evidence of both ignorance and negligence over the use of company IT resources. One in five workers let family and friends use company laptops and PCs to access the Internet. More than half connect their own devices or gadgets to their work PC and a quarter of these do so every day. Around 60 percent admit to storing personal content on their work PC. One in ten confessed to downloading content at work they shouldn't. Most errant workers put their firms at risk through either complacency or ignorance, but a small minority are believed to be actively seeking to damage the company from within. Five percent of those questioned say they have accessed areas of their IT system they shouldn't have while a very small number admitted to stealing information from company servers." < http://tinyurl.com/8rjz5 >

In the previous section, I presented an example of careless or ignorance that can bypass technical security. I pointed out that combining the unthinking use of REPLY ALL with visible distribution lists from a CC field can lead to violations of privacy even inside an organization. In this column, I want to finish my discussion with a few more points about the dangers of using visible distribution lists.

The problems caused by CC are worse when the recipients do not know each other. I have often received messages from technically unsophisticated correspondents who put dozens of e-mail addresses in the CC field even though many of the recipients are total strangers to each other. Such exposure of e-mail addresses always makes me nervous; who knows whether everyone on the list is trustworthy? Even if the list is not misused for outright spam, people often REPLY ALL with what I consider useless information, effectively adding me to a discussion list that I never wanted to be on.

One particularly annoying habit is to REPLY ALL with a joke stemming from some initial message. People then generate a series of increasingly long messages including copies of all the previous copies of the ostensibly clever repartee, driving me to generate an addition to my junk mail filter.

In one embarrassing case I was personally involved in, I added a new course developer to my MSIA faculty list and put the list name in the CC field by mistake in an all-points-bulletin. To my horror, the course developer cheerfully added my faculty members to a newsletter without permission. You can imagine the repercussions; there were two red faces that day and apologies to everyone.

The habit of using REPLY ALL is annoying enough when a reply does not in fact have to go to everyone on the original distribution list. However, REPLY ALL is a positive menace if it is coupled with the abhorrent practice of using an existing e-mail message as a shortcut to creating a new one with a completely different topic. Not only do many lazy users fail to modify the original message subject -- thus running the risk of having their new message ignored or filtered or misfiled -- but they may easily send sensitive information to the wrong people. This sloppy use of e-mail can result in gross violations of confidentiality.

In conclusion, you may want to put a note in your corporate security newsletter about the proper use of CC and BCC fields the next time you're casting about for a topic.

3 BURYING YOUR E-MAIL MESSAGE

As the end of the semester rolled around at Norwich University, my special-topics students were busily sending their examining committees their final reports. One lad – let's call him "Albert Baker" – noted that he was re-sending his report because one of his examiners mentioned that he hadn't received it; the student apologized for possible duplicates.

I responded that I hadn't seen it either.

An hour later, I opened an e-mail message from a sender I didn't recognize; albert@biepald.com (all names and addresses have been changed to nonexistent ones). The topic was "C'est fini" or "it's done" in French. I had left this message in my in-basket for some time because I always open messages with obvious subject lines and from people I know before dealing with reader correspondence, messages from strangers, or possible junk e-mail.

The mysterious message turned out to be from Albert and included the missing report. Had he sent it from his Norwich account, which would be bakera@norwich.edu, or at least included his real name, I would have opened it sooner. Had he used a meaningful subject line, such as "IS406 Final Report," it wouldn't have sat there unopened for so long.

This incident got me thinking about the current overload of e-mail that so many of us are suffering and what it means for effective use of this communications channel.

From a security standpoint, sending e-mail that doesn't get opened is a breach of security: it violates the principle of utility. What's the use of sending a message that gets ignored? Or at least, that gets ignored longer than it should? That slowdown could be viewed as a breach of availability of the message.

So here are some simple suggestions that you can circulate among your colleagues in your next newsletter to help improve the usefulness and timeliness of e-mail that matters – by which I mean e-mail that is work-related and needs a response:

1) Configure your e-mail client to include your real name, not a blank or a pseudonym. Your e-mail address can be anything you like; just be sure that you don't send people e-mail whose only identifier is something like bob123@genericemail.net .

2) Use a meaningful subject line. Don't be cute: "Something sweet for you" is more likely to be dumped in the spam/porn receptacle than opened in these days of swarming unwanted e-mail.

3) Don't use the FORWARD or REPLY function of your e-mail to start a completely new topic. Especially if the topic you've been discussing is low priority and your subject line just continues using that string instead of indicating a new, more important topic, don't be surprised if some of your recipients assign low priority to your new message, too. It can be disconcerting to open a message apparently discussing, say, "Refund policy for out-of-town expenses" and discover that it's actually dealing with what should have been labeled, "Emergency faculty meeting called for 15:00 today" – especially when you open the message the day after the meeting.

4) Be modest: not everything you say or find interesting is worth sending to everyone you know. Contrary to the apparent belief of some egoists, their colleagues do not in fact sing Sting's "Every breath you take" song as they wait expectantly for the next "Me too" or "Yeah! Right on! You go, girl!" comment appended to 12 pages of copies of copies of copies of some two-week old message they've already seen 32 times. Send too much junk and all your mail will be relegated to the virtual dust bin.

This last point bears a little elaboration. At one point, someone in my University decided to send the entire faculty a "Thought for the Day" consisting of some cute quotation. Well, I pretty quickly added that person's e-mail address to my "PLACE IN JUNK E-MAIL FOLDER" filter. Unfortunately, the same person was responsible for sending out faculty notices that really did matter, so I ended up having to check all this rubbish anyway. Someone must have complained, because the junk did eventually stop.

OK, now if this were junk e-mail, it would end "SEND THIS TO EVERYONE YOU KNOW!!!!"

But it isn't (I hope).

4 FORWARDING E-MAIL

A reader from Singapore wrote,

"I would like to know what are your views on email forwarding; i.e., should staff be allowed to forward mails to their external accounts (Internet mail accounts)? I work in a hospital and I have request from Doctors who asked that the auto-forward feature of their Lotus Notes e-mail messages be enabled to forward their e-mail to their external Internet mail account so that they can read it while at home or overseas. There were some security concerns here that confidential mails would then end up circulating in the Internet."

This question forces us to confront the conflict between theory and practice. E-mail and other traffic on the Internet has no inherent confidentiality. In theory, anyone capable of intercepting

TCP/IP packets anywhere during transmission can breach confidentiality. Thus, again in theory, anyone with access to the equipment of Internet Service Providers, Internet backbone transmission lines, and even to the public switched telephone network can intercept packets. With downlink footprints from satellite relays amounting to square miles, practically anything can in theory be intercepted from much of the traffic circulating on the Internet.

However, in practice, reported breaches of confidentiality have almost all resulted from data access at the end points, not in transit. Insider attacks and breaches of server security have been responsible for most of the data interceptions that have reached the press and the courts.

A practical impediment to effective interception of meaningful data in transit is the datagram routing that underlies the Internet: datagrams are packets of information with origin and destination information; store-and-forward transmission allows these datagrams to be sent through the Internet via different routes from other packets in a message stream. Routing tables can be updated in real time to reflect changes in traffic density or availability of specific links to other destinations on the Internet, so there is no guarantee that packets from the same message will travel the same route or arrive in the proper sequence (sequence numbers allow reassembly of the original message). Therefore seizing individual packets at random anywhere other than the origin and destination of packets is unlikely to result in very much result for the effort.

Nonetheless, best practices do recommend that encryption be used for communication of sensitive data; therefore, many organizations install Virtual Private Networks (VPN) for communication with established trading partners. VPN software is also available for "tunneling" through the Internet from a remote workstation over non-secure communications lines. A simple example of such a link-encryption function is the Web-based e-mail services that use SSL to establish a secure link to the e-mail server (i.e., they use HTTPS instead of just plain HTTP). The user can pick up e-mail from the corporate server without having it forwarded in the clear to an insecure external e-mail service. Some of the e-mail products include facilities for direct communication between a secure e-mail servers and the users' e-mail clients.

Using "VPN tunneling software" as a search string in the GOOGLE search engine brought up hundreds of hits, many of them for specific products and data sheets, so I am sure you will be able to find a solution that fits your needs.

In your specific case, the fact that some of the e-mail might include confidential patient data means that the relatively modest investment in VPN technology would make a lot of sense for you in complying with your local legal requirements for protecting such data. But once you have the VPN in place, please make sure that all your users have also implemented driver-level data encryption on their computers so that the received, decrypted data are not susceptible to discover if someone steals their laptop or home computer.

5 E-MAIL SUBJECT LINES EXPLOITED BY WORMS

This morning I received a bounce for an e-mail that I didn't send.

Now, partly because I don't like opening potentially executable code automatically, I don't use POP mail, so it is not feasible for a worm to launch infected messages from my system; in addition, my Norton Anti-virus (NAV) is automatically updated, so it's unlikely that I would be infected. Finally, I don’t open unexpected attachments in native (executable) mode: I use a utility (Keyview, in my case) to examine the content as text. So this is what I saw in the text of the “bounced” message:

* * *

```
Date: 9 May 2002 16:36:40 +0800
--RuADZVmR31l68x591fL6
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable
<HTML><HEAD></HEAD><BODY>
<FONT>The following mail can’t be sent to
chnserv@globalsources.com:<br>
<br>
From: mkabay@compuserve.com<br>
To: chnserv@globalsources.com<br>
Subject: how are you<br>
The file is the original mail</FONT></BODY></HTML>
--RuADZVmR31l68x591fL6
Content-Type: application/octet-stream;
 name=most.exe
Content-Transfer-Encoding: base64
Content-ID: <T57z06Z4>
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
. . . . 8><= [SNIP] . . . .
```

* * *

Hmm, I hadn’t sent any messages with subject “How are you” and there is no one in China (.cn) that I’ve written to recently anyway. So prima facie, this is likely to be a forged header. Sure enough:

```
* * * HEADER ANALYSIS USING SAMSPADE v1.14 * * *
Sender: wangjl@dsp.ac.cn
Received: from dsp-ns.dsp.ac.cn ([159.226.219.1]) by
 siaag1aa.compuserve.com (8.9.3/8.9.3/SUN-1.12) with ESMTP
 id EAA18353 for <mkabay@compuserve.com>; Thu, 9 May 2002
 04:07:45 -0400 (EDT)
 This received header was added by your mailserver
 siaag1aa.compuserve.com received this from someone claiming
 to be dsp-ns.dsp.ac.cn
 This host doesn’t exist, so all headers below this one
 are probably forged
Received: from Uhpoooz ([159.226.219.34]) by
 dsp-ns.dsp.ac.cn with Microsoft SMTPSVC(5.0.2195.2966);
 Thu, 9 May 2002 16:36:40 +0800
 dsp-ns.dsp.ac.cn received this from someone claiming
 to be Uhpoooz
 This host doesn’t exist, so all headers below this one
 are probably forged
From: postmaster <postmaster@compuserve.com>
To: mkabay@compuserve.com
Subject: Returned mail--”how are you”
MIME-Version: 1.0
Content-Type: multipart/alternative;
 boundary=RuADZVmR31l68x591fL6
Message-ID: <DSP-NSNYgEj4v5iJarn00000cfb@dsp-ns.dsp.ac.cn>
```

```
X-OriginalArrivalTime: 09 May 2002 08:36:40.0549 (UTC)
 FILETIME=[A408E150:01C1F734]
Date: 9 May 2002 16:36:40 +0800
```

* * *

Many other worms use misleading subject lines; for example, the Melissa.I variant of the notorious Melissa worm uses any of eight different subject lines:

- Question for you
- Check this!
- Cool Web Sites
- 80mb Free Web Space!
- Cheap Software
- Cheap Hardware
- Free Music
- Free Downloads

SIRCAM goes one better by using the name of the attached infected document (minus the file suffix), thus providing an infinite variety of subject lines.

Finally, a quick note on a curious reversal of the well-known hoax warnings that circulated years ago such as the following, described at < http://www.europe.f-secure.com/hoaxes/returned.shtml >:

```
There is a new virus going arround [sic] in the last couple of
days!!! DO NOT open or even look at any mail that you get thar
says: “Returned or Unable to Deliver” This virus will attach
itself to your computer components and render them useless.
Immediately delete any mail items that says this. AOL has said
this is a very danderous [sic] virus, and there is NO remedy for it
at this time, Please Be Careful, And forward to all your
on-line friends A.S.A.P.
```

Ironically, the message I received about a bounced e-mail really did include malicious code in the attachment.

Moral: don’t trust the subject line of *any* e-mail message that has an unexpected attachment.

Other guidelines:

1) Before you open any e-mail message that includes an attachment, examine it to see if you recognize the sender; be suspicious if you don’t.

2) Before sending anyone an attachment of any kind, ensure that the recipients know what’s coming to them and in what format.

3) Do not send anyone executable files of any kind; if, exceptionally, you have some extraordinary reason to send executables, convert them to a non-executable form and then sign the converted version digitally (e.g., using PGP), then follow rule (2).

And the ever-popular general principles,

4) Choose antivirus products that can update themselves automatically and make sure they do so.

5) Enable automatic scanning on file open and file save.

6) Scan your entire system regularly (I configured NAV to scan all disks at one in the morning every Saturday night).

6 INTERNET E-MAIL AND THE FIREWALL

External e-mail of all kinds can be filtered through a firewall system which strictly controls the addresses of inbound and outbound messages. Specifically, such a firewall must include detection of fraudulent addresses on inbound e-mail: addresses implying that external e-mail originated from within the organization. For consistency, and as a service to the greater community, such a firewall should also restrict outbound e-mail to ensure that no such messages have addresses implying that they originated outside the organization. These measures help to fight unsolicited commercial e-mail ("spam") on the Net.

Management Implications of External Access

All e-mail sent outside the organization by internal users raises important issues about authorized functions and the image of the organization in the outer world.

E-mail Access to FTP

Although e-mail-only gateways are feasible to allow users to exchange messages with other users in the wider world, it must be mentioned that there are ways for users to perform unauthorized functions such as file transfers simply using e-mail. E-mail FTP servers receive search or file-transfer requests (scripts or batch files) by e-mail and carry out those instructions anywhere on the Internet. The server then packages the results of the file transfer (or search, etc.) and sends it back to the originator as an e-mail message. Binary files are converted using MIME, UUENCODE, PGP or other transformation to 7-bit ASCII. This mechanism thus provides a covert channel for receiving binary files without going through normal security restrictions imposed on the import of executables.

Another form of binary file that may cause considerable embarrassment to the organization is graphics. There have already been several cases in the United States in which government workers have been discovered using official computer resources to retrieve, store and exchange pornographic and other undesirable materials. The consequences for several employees and their managers have been severe.

In addition, USENET discussion or news groups can be joined using e-mail. Subscribers receive information about specific subjects of interest as ordinary messages and can reply if the system provides outbound Internet e-mail. Given the wide range of topics available in the USENET, it is important to establish which news groups may be joined by users. Many of the news groups cover highly technical areas (although the signal-to-noise ratio tends to be low) and are legitimate sources of information for special purposes. However, many news groups (especially those in the alt. category) are of questionable value to the work of organizational employees. Some news groups would be extremely undesirable: those dealing in extremist propaganda, organized hatred, and pornography would be embarrassing for the organization if there were to be organizational subscribers.

Such activities must be carefully controlled and will require explicit policies to prevent abuse. If intelligence gathering requires monitoring of such groups, analysts should subscribe using IDs not traceable to the organization.

Denial of Service

The sheer volume of inbound e-mail resulting from uncontrolled subscriptions to news groups may flood a system's communication capacity and, if stored on-line, may occasion significant costs for disk storage. Useless e-mail should be purged periodically as a normal function of system house-keeping.

7 ORGANIZATIONAL E-MAIL ADDRESSES

The previous section deals with inbound e-mail from Internet/USENET news groups.

However, it is important to realize that any outbound contribution to any news group or other discussion group in cyberspace by a user will be identifiable as coming from the employer's organization simply by the user's e-mail address. This implies that every message sent out of the organization into the Internet must be considered as potentially damaging to the interests of the organization.

The opposite is also true: professional, helpful contributions by individuals affiliated with an organization enhance the organization's image and reputation.

The organization must frame and implement clear policies on participation in such news groups. For users authorized to participate in selected groups, the organization must provide training on appropriate "netiquette" to ensure that employees consistently project their professionalism. It would be embarrassing for the organization, for example, to discover that an employee had "flamed" another user (sent offensive e-mail) using their corporate ID. Attempts to absolve the employer from blame by adding cute signature lines are futile: no one believes that someone with an ID of ralphm@megacorp.com is criticizing a competing product without knowing that MegaCorp will be assumed to support his attacks.

E-mail users, even polite and professional ones, are subject to mail-bombing runs by disgruntled or mischievous Internet users. For example, two lawyers who sent out thousands of e-mail messages by "spamming" the Internet with advertisements for their Green Card advisory services in the early 1990s were deluged by messages from angry users around the planet, bringing their Internet access provider's servers to a halt.

In another incident, a naive sales manager posted two dozen similar commercial messages in what he thought were appropriate news groups; angry Internet users then posted his company's 800-number in various recreational sex groups in the "alt" domain, describing them as free sex-chat lines.

The resulting wave of offensive phone calls caused one of the receptionists to resign in disgust and completely swamped the inbound 800 service and denied service to legitimate customers. The company decided that they could not afford to change their 800 number, so they had to suffer through the loss and embarrassment of the episode until the calls died down.

In my own case, I locked a rude user out of the NCSA Forum on CompuServe around 1993 after repeated warnings not to use vulgarity or to attack other participants. As a result, I suffered through a couple of months of rambling, obscene verbal assaults — and so did about 50 other people to whom the disturbed individual sent copies. He eventually had to be removed from CompuServe altogether.