Using Email Safely and Well

Version 8 (July 2016)

M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

Contents

Download this file from

http://www.mekabay.com/infosecmgmt/emailsec.pdf

1 FIRST E-IMPRESSIONS

When you receive an email message from a stranger, do you care whether it has spelling mistakes and grammar mistakes? What about offensive language and off-color humor? Does the context matter? For example, do you apply the same standards to email referring to business matters and to informal communications about, say, a hobby or interest?

Researchers at the University of Chicago have been investigating the effects of email on perceptions of character. According to a summary by Cathy Tran in *Science Now* < http://sciencenow.sciencemag.org/cgi/content/full/2005/719/1 (by subscription only) >, psychologist Nicholas Epley and colleagues examined conversations carried out exchanges on conversational topics by phone between randomly selected people using six assigned questions. They then transcribed the answers and used them for the email version of the Q&A sessions.

Their results were interesting. The questioners had been given false biographical sketches of the people they were communicating with indicating substandard intelligence or normal intelligence as well as different pictures showing neat people or slobs. Questioners who used the phone to listen to the prescribed responses had favorable impressions of their interlocutor's intelligence regardless of the bios and pictures. In contrast, "Via email, however, students held onto their first impressions, continuing to assume their partners had substandard intelligence, for example, if that's what the biographical sketch indicated."

If this research is confirmed, I think the lesson for us is that when using email, first impressions really do count. Professionals should carefully review email messages for acceptable writing, including word-choice, punctuation, capitalization, and spelling.

Looking like an idiot is easy; correcting that impression via email may not be so easy.

2   DISCRETION IN EMAIL CRITICISM

Today I want to touch on awareness about email protocol and specifically discretion in sending off-the-cuff critical comments to someone via corporate email.

All of us encounter times where we disagree with something our colleagues are saying or doing; however, not every impulse to respond should lead to an official email: those should be regarded as on-the-record communications that may be interpreted – and misinterpreted – by others in the organization who may jump to conclusions that are unwarranted.

Let's take a look at a scenario and analyze what's happening.

Albert sends Bob an email message addressed only to Bob. In it, Albert speculates about possible business strategies for their employer. Bob disagrees with his perception of the suggestion and writes a highly critical memo back to Albert using the company's email. However, it turns out that either through unclear writing from Albert or misunderstanding by Bob, the information and assumptions detailed in Bob's response can easily be viewed as indicating that Albert is undermining the interests of his own employer.

What are the possible sources of disagreement whenever people don't see eye to eye?

- They may differ in fundamental assumptions;
- Their vocabulary may differ: they use words differently;
- Their unspoken goals and values may differ;
- Their implicit reasoning may differ;
- They may lack essential shared information;
- They may have made a mistake in observation, reasoning, or articulation of their views.

What are some of the elements that lead to a perception of impoliteness in communications? In a 2008 book called *Impoliteness in Interaction*< http://www.amazon.com/Impoliteness-Interaction-Pragmatics-Beyond-New/dp/9027254397/ >, Professor Derek Bousfield< http://www.uclan.ac.uk/ahss/journalism_media_communication/derek_bousfield.php >, PhD, Head of Linguistics, English Language, Literature & Culture at University of Central Lancashire< http://www.uclan.ac.uk/ > in England analyzes elements of impoliteness using detailed records of less-than-pleasant interactions. In Chapter 6, "The dynamics of impoliteness I," he discussed several stages and levels of impoliteness. Elements he analyzes[1] in detail include (examples are my own):

- Pre-impoliteness sequences: words and phrases that set the stage for aggressive or defensive speech; e.g., "I'd like to ask you…." Or "Listen to me...."
- Repetition of challenges: rapid sequences of accusatory language that emphasizes hostility; e.g., "Don't you think that…. Isn't it obvious that…. Why can't you see that…."
- Insertion of taboo words: obscenities, shocking images; e.g., "Why the **** can't you see that…." or "What's the matter with you, you have your head stuck up your ***?"
- Derogatory nominations: demeaning descriptions of the interlocutor or of ideas; e.g., "You're a real [insert insult here] sometimes" or "Well that idea is really off the wall."
- Forcing feedback: demanding a response at the end of a hostile interaction; e.g., "Why did you do that?" or "So what are you going to do about it?"

---

[1] My thanks to Norwich student Chase Hammer for pointing out the original typographic error, in which I wrote "analyses."

In my experience, many people don't edit their email messages at all before sending them; some don't even check their spelling. Under those circumstances, an email that seems like a collection of blurted-out insults can make any situation worse.

I think that any time we find ourselves starting to use hostile expressions in our email, it's time to stop and think:

- Will this interaction contribute to solving a problem or will it make it worse?
- Would it be better to meet the interlocutor face to face instead of relying on email?
- Failing that, can we use a video link (e.g., Skype) to discuss the issue with a modicum of body-language that can clarify feelings instead of letting them be guessed from written, often poorly-edited, spontaneous reactions in email?
- If video isn't available, can we at least telephone the interlocutor or use voice over IP tools for the interaction? At least there will be verbal cues about the feelings involved.
- If none of the live-contact interactions are available, is instant messaging available, with its menus of emoticons that can provide clarification of emotional context – and lead to rapid interaction point by point instead of forcing a delayed response to an extensive message?

A true story from one of my students illustrates the danger of stupidly sending offensive remarks by email – especially in a REPLY ALL, as will be discussed later in this collection of essays. It seems that one of our Norwich students was an intern at a large company one summer when he and everyone else in the company received a message from the CEO of the company on the second day of the internship; the message included a question. A fellow intern – NOT a Norwich student! – wrote something along the lines of "That's the stupidest question I've ever read" and hit REPLY ALL. He was fired that afternoon.

In my email client, I have a 30-minute send-cycle; unless I cause an immediate SEND, my email sits in an outbox for a while before it gets sent. Those minutes of buffering have saved me from errors of content and of judgement; perhaps they will be useful to you too. Sometimes I deliberately write a horrible, insulting and funny response to something, laugh about it, and then immediately delete it before it is sent.

Think carefully about the responses your message will elicit; work for collaboration and cooperation, not conflict by default.

The cardinal rule I have used for decades is, "**If you're angry, don't send the email until you've cooled down and thought about it.**"

3 HTML-FORMATTED EMAIL DOESN'T WORK RELIABLY

One of the six fundamental attributes of information that we protect is integrity, one aspect of which is consistency with the originally stored data. When someone goes to the trouble of producing an elegantly formatted memorandum or other document and sends it out to recipients, everyone would like to preserve data integrity by seeing the same appearance on all the systems sharing that document.

Unfortunately, sending formatted messages as email messages (as distinct from attachments) *does not guarantee* preservation of the exact appearance of the source material.

Attractive, well-formatted email messages with boldface, italics, different point sizes and the like usually get transmitted as HTML (hypertext markup language) to recipients' mailboxes, where most people's email clients (Eudora, Netscape, Outlook and so on) allow the funny-looking code to be reconstituted into something similar to the original.

I say "similar" rather than "exactly like" because HTML does not necessarily control the final appearance of text on a recipient's system. The codes refer to types, not exact matches, of fonts; thus a sender might want to use, say, 24-point Arial as a Heading 1 display but a particular recipient might have defined Heading 1 as, say, Times Roman 14 point. A two-page original document may appear to be a three-page document to one recipient and a one-page document to another recipient.

More significantly, though, many people turn off HTML email for security reasons. All such formatted email gets converted automatically into plain ASCII text. The fragment of message below (demarcated by the > and < symbols) is in plain text as I received it:

```
Note: The on-line course evaluation system may be used from room, lab
and home ? anywhere Internet access is available.

Overview: . . . . Failure to complete a course evaluation will result
in a ?hold? being placed on the student?s final grades.
```

When this message was auto-converted to ASCII, the apostrophes turned into question marks – probably because the writer was using "curly" characters instead of the straight ones in your word-processing package or email editor. If you care to prevent this peculiarity (if you're using Word), turn off the option in the {TOOLS | AUTOCORRECT | AutoFormat As You Type} screen: uncheck the box labeled {"Straight quotes" with "smart quotes"}.

In addition, it looks like a dash character may have been in the text in the first line (labeled "Note"). One can turn that conversion off in the same menu by unchecking {Hyphens (–) with dash...}.

Some people try to send files that should look the same on a recipient system and the originating system by attaching word processing documents; e.g., Word DOCX files, WordPerfect WPD files, Rich Text Format (RTF) files, OpenDocument Texts (ODT) files (and so on). Unfortunately, even these attempts don't necessarily work as planned, since many factors may cause the documents to be unusable or to look different on different systems:

- Lack of specific application programs
- Lack of shared fonts
- Different default paper sizes (different countries may use different sizes)
- Different printing margins (resulting from installation of different printers).

So if the exact appearance of a message you are sending via email is critically important to you, you can send the content *and* its format in a way that is (largely) platform independent: attach an Acrobat PDF (Portable Document Format) files. Although even they don't necessarily result in perfect rendition of the author's intentions across systems, PDF files are far more likely to succeed than the other methods mentioned above.

You can create PDF files in a number of ways; some systems have PDF output functions installed so that you can either "print" to a PDF driver to create the PDF files or even just click a SAVE AS PDF toolbar button to do so from within your word processor, spreadsheet and so on. Other packages exist that are less expensive (and generally less feature-rich) than the full Adobe Acrobat software but nonetheless allow users to create PDF files easily. Type "create PDF" into a Web search engine to find lots of choices.

One other note about PDF: if you are sending information you created in a spreadsheet such as Microsoft EXCEL and you do not expect your correspondents to *change* the results of your work, you are far better off sending a *printout* of your results using a PDF version than sending the spreadsheet itself:

- Not everyone can open a spreadsheet file
- Many people have no idea how to work with a spreadsheet even if they can open it
- Clumsy or novice users may modify the data or formulae in a spreadsheet without realizing that they are damaging the information you sent them and looking as misleading results
- Spreadsheet programs and files are noticeably slower to load than Acrobat readers and PDF files.

So get used to thinking in terms of reliable, portable documents when you send information to others.

4   CC + REPLY ALL = TROUBLE

CONTROL VISIBLE DISTRIBUTION LISTS IN EMAIL

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 email addresses into the CC (carbon copy) field 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 field for addresses to a distribution list.
- Many people unthinkingly use REPLY ALL for replies to every email 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 email 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 email and count how many obvious cases there are of emails with inappropriate subject fields and inappropriate distribution lists sitting in your received-folders. I think you will be dismayed by the results of your research.

5   BCC PREVENTS EMAIL 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 email addresses in the CC field even though many of the recipients are total strangers to each other. Such exposure of email 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 email 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 email can result in gross violations of confidentiality.

So remember:

- TO: field for people directly involved in the correspondence and to whom replies are required for action or response
- CC: field for people who need to know about the correspondence and to whom replies are helpful but who are not expected to respond unless they have specific information or comments
- BCC: for people who need to receive a widely distributed announcement but who should not receive commentary sent back to the originator(s) of the original message
- Remove unnecessary information (such as chains of previous correspondence) from a message to which you are replying or which you are forwarding before sending it.

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.

6   BURYING YOUR EMAIL 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 email 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 fields and from people I know before dealing with reader correspondence, messages from strangers, or possible junk email.

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 field, 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 email that so many of us are suffering and what it means for effective use of this communications channel.

From a security standpoint, sending email 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 email that matters – by which I mean email that is work-related and needs a response:

- **Configure your email client to include your real name, not a blank or a pseudonym.** Your email address can be anything you like that conforms to your organization's policies; however, if you are using private email, be sure that you don't send people email whose only identifier is something like bob123@gmail.net .

- **Use a meaningful subject field.** 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 email.

- **Don't use the FORWARD or REPLY function of your email to start a completely new topic.** Especially if the topic you've been discussing is low priority and your subject field 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.

- **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 < https://www.youtube.com/watch?v=cEnJDaqT3-0 >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 email address to my "PLACE IN JUNK EMAIL 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 email, it would end "SEND THIS TO EVERYONE YOU KNOW!!!!"

But it isn't (I hope).

7   MISLEADING SUBJECT FIELDS

Two of the six fundamental attributes of information that information assurance is supposed to protect are utility and confidentiality. In this section, I want to address damage to utility and confidentiality resulting from two of the most common errors in using email: mislabeling the subject and making the addresses of everyone in the distribution list public.

Many people make the mistake of creating new messages to a correspondent by finding any old message from that person and replying to it. The problem is that these people usually leave the old subject intact, resulting in ridiculous situations such as finding a critically important message in July in an email labeled, "Birthday party 12 May."

Not all email messages are created equal; some are destined for the trash heap, if not of history, at least of the email system. That decision is sometimes made automatically as a function of the subject field. For example, I usually flag email messages that have resulted from jokes and that consist of additional comments tacked to the top of ever-expanding copies of previous messages. Once I add the subject field of these messages to my filter, my email program automatically routes the jokes to a junk mail folder. Anyone inserting operationally important information into such a data stream is out of luck.

Another problem with mislabeled subjects occurs when someone embeds more than one distinct topic in an email message whose subject field implies otherwise. For example suppose an email message subject reads "Next week's meeting" but the sender includes an urgent request for action today on some critical issue; there's a good chance the receiver may not open the message right away if other messages seem more important.

Try to make your subject field as descriptive as possible without turning it into a paragraph. Some email systems truncate subject fields in the display of messages that a user sees; it makes sense to put keywords at the front of the subject. I encourage my staff to use prefixes such as "MSIA:" or "ACCREDITATION:" to help organize our messages.

Using standard formats in subject fields can help, too. For example, in our work in the MSIA, I have asked that faculty and staff referring to an issue in a particular seminar use the form "MSIA c.s" in their subject field, where c represents the class (e.g., 7 for students starting in September 2005) and s represents the seminar number (thus MSIA 7.3 for seminar 3 in the MSIA 7 class).

I ask undergraduate students always to start their emails to me using the class ID (e.g., CS120) so that I don't have to look up which class they may be in! That practice also allows me to grab a bunch of messages from my INBOX and file it in the appropriate course folder in one operation.

In summary,

- Use an appropriate agreed-upon prefix in the SUBJECT if possible
- Use a properly descriptive SUBJECT field
- Don't REPLY to an old message on a different topic and then leave the old SUBJECT and a copy of the original message
- Don't mix separate topics in a single message.

8   EMAIL DISCLAIMER STIMULATES EXPLETIVES

One year, I received a 30-word email message from a very nice reader in Britain and noticed that his email system added the following astonishing disclaimer, which I quote in its sonorous totality after scrubbing it of identifying details:

```
This email, its contents and any files or attachments transmitted with
it are intended solely for the addressee(s) and may be legally
privileged and/or confidential. Access by any other party is
unauthorised without the express written permission of the sender.
If you have received this email in error you may not copy or use the
contents, files, attachments or information in any way nor disclose the
same to any other person. Please destroy it and contact the sender on
the number printed above, via the <Name of Bank> switchboard on +44 (0)
nnnn nnnnnn for <place1> and + 44 (0) nnnn nnnnnn for <place2> or via
email by return.

Internet communications are not secure unless protected using strong
cryptography. This email has been prepared using information believed
by the author to be reliable and accurate, but <Name of Bank> makes no
warranty or representation, express or implied, as to its accuracy or
completeness and is not liable to you or to anyone else for any loss or
damage in connection with any transmission sent by the Bank to you over
the Internet. <Name of Bank> makes no warranty that any information or
material is free from any defects or viruses.

In particular <Name of Bank> does not accept responsibility for changes
made to this email after it was sent. If you suspect that this email
may have been amended or intercepted, please contact the sender in the
manner stated above. If this transmission includes files or
attachments, please ensure that they are opened within the relevant
application to ensure full receipt. If you experience difficulties,
please refer back to the sender in the manner stated above.
Any opinions expressed in this transmission are those of the author and
do not necessarily reflect the opinions of the Bank and may be subject
to change without notice.

Please note that for the purposes of this document all references to
<Name of Bank> or the Bank shall be taken to mean <Name of Bank>
(place) Limited or any other member of the <Bigger> Bank Group. Nothing
in this transmission shall or shall be deemed to constitute an offer or
acceptance of an offer or otherwise have the effect of forming a
contract by electronic communication.
```

 I commented in my response to my correspondent, "Did you know that your message has 30 words (152 bytes including spaces) whereas your disclaimer has 367 words (2177 bytes)? That's the lowest signal-to-noise ratio (6.5% useful info out of the total and a 72.6:1::noise:signal ratio) I've ever seen outside a copy-of-copy-of-copy chain. Please congratulate your attorneys on making maximal use of bandwidth!"

Really, this disclaimer does seem excessively detailed to me. If the same level of legalistic caution were applied to phone calls, it would make a wonderful Monty-Pythonesque skit:

"OK then, I'll see you at lunch tomorrow."

> "Yep, but wait – you have to listen to the automated legal disclaimer our attorneys have programmed into our phone system. Just hang on [buzz, click]. [metallic voice] This phone message is intended solely for the recipient(s) and may be legally privileged and/or…." [CLICK!]

Or what about introducing this degree of caution into face-to-face interactions?

> "So how do you want your hot-dog, with mustard and relish or without?"

> "With both, please. And this verbal instruction is intended solely for the recipient(s) and may be legally privileged and/or…."

On a more serious level, cluttering up email messages this way is a waste of bandwidth. It's worse in offices where people copy entire messages without editing the contents, resulting in copy-of-copy-of-copy chains that spread like cancerous eruptions through inboxes throughout the organization. I have personally seen messages that are 20 levels deep, all of them including the headers, salutations, copies of previous messages and disclaimers in a long string of garbage contributing nothing whatever to enlightened discourse. Some well-meaning folks even include the detailed headers in their copies.

As a matter of courtesy and good sense, when one replies to a message, it's a simple matter to strip non-essentials out of the copy of the original. I use ellipses (… for cuts within a sentence, …. for cuts crossing sentence boundaries) to signal gaps, but usually one or two snips are enough to clean up the copy so that the reader can get the gist of the conversation without having to wade through reams of superfluous stuff.

So the next time you encounter a huge disclaimer laid like an unsightly pile of refuse at the bottom of a colleague's email message, you can use a slightly modified British expression in your response: "UNSTUFF IT!"

9 FORWARDING CORPORATE EMAIL

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 email messages be enabled to forward their email 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. Email 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 email services that use SSL to establish a secure link to the email server (i.e., they use HTTPS instead of just plain HTTP). The user can pick up email from the corporate server without having it forwarded in the clear to an insecure external email service. Some of the email products include facilities for direct communication between a secure email servers and the users' email 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 email 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.

Page 17 of 34

10   EMAIL CARRYING MALWARE

One morning I received a bounce for an email that I didn't send.

Now, partly because I don't like opening potentially executable code automatically, I don't use HTML-enabled email, so it is not feasible for a worm to launch infected messages from my system; in addition, my BitDefender antivirus 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//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
. . . . 8><= [SNIP] . . . .
```

* * *

Hmm, I hadn't sent any messages with subject "How are you," there is no one in China (.cn) that I've written to recently, and I block all unknown writers from most top-level international domains involved in heavy spam-generation (e.g., .cn, .ru, and so on) 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 fields; for example, the Melissa.I variant of the notorious Melissa worm uses any of eight different subject fields:

```
    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 fields.

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 email really did include malicious code in the attachment.

Moral: *don't trust the subject field of any email message that has an unexpected attachment.*

Other guidelines:

- Before you open any email message that includes an attachment, examine it to see if you recognize the sender; be suspicious if you don't.
- Before sending anyone an attachment of any kind, ensure that the recipients know what's coming to them and in what format (so they can open it)
- Do not send anyone executable files of any kind by email; 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). Many email systems automatically block sending and receiving executables.

- Name every file you are sending in a descriptive way;
  e.g., **2016-01-16_weekly_opsec_report.pdf** rather than **a3948vm7.pdf** .

And the ever-popular general principles,

- Choose antimalware products that can update themselves automatically and make sure they do so.
- Enable automatic scanning by your antimalware product on every file-open and file-save.
- Scan your entire system regularly for malware infections (I configure my antimalware software to scan all disks at 01:00 in the morning every Saturday night).

11   EMAIL FROM THE ORGANIZATION

External email 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 email: addresses implying that external email originated from within the organization. For consistency, and as a service to the greater community, such a firewall should also restrict outbound email to ensure that no such messages have addresses implying that they originated outside the organization. These measures help to fight unsolicited commercial email ("spam") on the Net.

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

Although email-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 email. Email FTP servers receive search or file-transfer requests (scripts or batch files) by email 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 email 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 email. Subscribers receive information about specific subjects of interest as ordinary messages and can reply if the system provides outbound Internet email. 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.

12   ORGANIZATIONAL EMAIL ADDRESSES

The previous section deals with inbound email 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 email 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 email) 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.

Email 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 email 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.

13 THE KEEPER OF THE LISTS

The College of Graduate and Continuing Studies at Norwich University is large enough that there is significant turnover among the staff. Until recently we were we adding new staff members periodically and we also move staff members from one group to another; for example, a staff member might change from being an assistant director in one program to being an administrative director in another. Occasionally we also have staff members who leave the group or even the University altogether.

One of our staff members (the Keeper-of-the-Lists or KL) maintains the list of all of our staff members; however, there is no link between the XL file she maintains and the mailing lists that each member of the CGCS must maintain to be able to distribute email to appropriate groups. I remember one time, I noticed that on all-CGCS mail message sent by a colleague seemed to have an abnormally short distribution list. Sure enough, when I checked the names, I found seven errors: two missing deletions and five missing additions. One of the undone deletions was the name of a staff member who no longer works at the University at all.

Trying to make dozens of people (as of January 2009 we had 41 staff members) maintain several distribution lists is a hopeless cause: even with the best will in the world, people will inevitably forget to update their lists and therefore

- Some mailings will miss legitimate recipients;
- Some people will receive messages they have no business reading.

There are at least four solutions that would rectify this problem.

- We could use the Yahoo Groups function to define closed groups under the control of the Keeper-of-the-Lists; these provide automatic access to mailing lists (this was an utter kludge and I didn't like it because we would be putting our faith for continued production application in a free resource completely out of our control).
- IT could install widely available list-server software to allow the KL to create and maintain specific lists; e.g. CGCS-ALL, CGCS-DIRECTORS, MSIA-STAFF, MSIA-INSTRUCTORS, etc. that all of us could use as addresses for email.
- IT could switch all CGCS users to any email client that supports exportable mailing lists (e.g., Outlook because we supported the rest of Office 2003). The KL could maintain and distribute updated corporate distribution lists. However, this solution would still require manual intervention by users: everyone has to replace their old list by the new list.
- IT could implement Microsoft Exchange Server, switch all CGCS users to Outlook 2003 and define corporate distribution lists maintained by the KL. All users would automatically access the one and only distribution list for each group without manual intervention.

Students reading this article should consider how the points apply to people running clubs and other groups at their college or university. Relying on individuals to coordinate their mailing lists of members or of executives simply doesn't work. Assign the task to a single person (with a backup for continuity of operations) and keep the lists up to date.

14   MAILSTORMS

Most of us belong to mailing lists; many of us have more than one e mail address; some of us use autoforwarding to shift e mail from one address to another automatically; and a few of us use automated responses on our e mail accounts to let correspondents know when we are out of the office or unable to respond quickly.

All of these factors can contribute to mailstorms.

A mailstorm occurs when computers begin sending mail to each other without human intervention and one or both have limited storage capacity for unread messages. Sometimes mailstorms can become a denial of service by saturating communications channels and other resources. The email enabled worms such as Melissa, the I-love-you message, and so on are examples of malicious software whose authors deliberately wrote them to create mailstorms.

Let's start with a simple situation which actually happened in the early 1990s:

- Sally goes on vacation and decides to receive her company e mail using an email service with a global presence but a limited capacity for unread emails, such as the old CompuServe or AOL services. She sets an autoforward command on her company account and sends all incoming mail to her more mobile CompuServe e mail account, figuring that she'll be able to log on from wherever she goes.
- Unfortunately, when she reaches the remote tropical island where she will spend her vacation, she discovers that it is impossible for her to access even her worldwide ISP without paying a surcharge of $6 a minute for long distance service to the mainland. She cheerfully shuts her computer and forgets all about e mail for the next three weeks.
- Meanwhile, back on the Internet, her company account dutifully forwards every message it receives to her CompuServe account. Unfortunately, Sally has forgotten that there is a limit of 250 messages on her CompuServe account and she reaches that limit within the first week of her vacation. At that point, every inbound message generates a bounce informing the sender that her CompuServe mailbox is full.
- The very first bounce message CompuServe sends her company account is cheerfully autoforwarded to her CompuServe account. So now that message generates yet another mailbox full message which then gets bounced back to her company account and so on without let up. Eventually, even her company mailbox fills up and then the two e mail systems continue chattering at each other indefinitely in a dialogue of demented robots.

The number of e mail messages that can be generated by this kind of infinite loop is a function of the latency of the positive feedback system that the user has accidentally created. For example, if it takes exactly one minute for a bounce message to be returned to the originating site, then each message causing an initial error can create sixty additional messages per hour. However, because new messages are arriving at the originating mailbox all the time, new sets of bounced messages are constantly added to the fun. It is not uncommon to see tens of thousands of messages accumulating in the recipient mailbox if nobody notices the loop.

There are several other mechanisms that inadvertently create mailstorms. For example, someone can accidentally autoforward e mail between two of their own accounts. Or suppose Albert and Betty both have full mailboxes; if either of these people sends an email message to the other, a mailstorm will result.

Suppose David has posted an automatic "out of office" response on his e mail address. If Charlene sends a message to David's e mail address and immediately enables her own out of office autoresponder message before David's response arrives, then David's autoresponder message spawns an equivalent response from Charlene's e mail and the mailstorm begins.

Imagine now that David belongs to a list where the FROM address is actually the broadcast address that sends his response to the entire list. You can see that his very first automated out of office response to the list will generate an infinite sequence of messages to and from that list. However, in this case, the entire population of the list will be receiving his autoresponse – very embarrassing for the list administrator and intensely annoying for everyone else.

Something analogous to a mailstorm results from thoughtless behavior when using a public list. I'm sure that all of us have experienced irritation when a list member posts personal comments obviously intended only for the poster of a public message and for no one else. For example, Mike asks for a list of readings and Norman answers on the list, "I'll send you a list tomorrow." Several thousand unwilling readers now know about this projected e mail message. One of these irritated people, say Orville, now posts a message to Norman saying, "Did you really have to post that message to the entire list?" Orville's message is so irritating to Paula that she now posts a message to the entire list criticizing Orville for criticizing Norman. And so the useless tempest of e mail continues via the public list, creating thousands of copies of useless information.

(While I'm on the subject of useless information, may I sneak in a request to everyone not to quote entire messages when responding to e mail? Just quote the small fragments of text that explain your responses. This principle is particularly important on public lists, where I have personally seen messages containing the entire text, including Internet headers, for up to seven levels of previous messages. In one study, I found that the signal to noise ratio of new information in a particular USENET group was only 5%; the rest was quotations of quotations of quotations *ad nauseam*.)

In conclusion, here are some simple suggestions for reducing the likelihood of mailstorms:

- Minimize the use of automated responses on your e mail accounts
- If you do autoforward your e mail, don't let your target mailbox fill up
- If you are receiving autoforwarded e mail from your primary mailbox, don't autoforward back to the original mailbox
- Email system administrators should receive exception reports identifying accounts with excessive numbers of email messages or excessive traffic so that they can investigate for mailstorms
- Firewalls that inspect the content of email message should be able to react to an excessive number of bounce messages from a single originating address and delete the traffic or inform system administrator of a likely mailstorm
- Managers of unmoderated lists should configure a FROM address different from the address that participants use to post messages to the list
- Users of list servers who want to send personal comments in response to posted messages should reply to the sender, not to the entire list.

15 DELIVERY NOT GUARANTEED

A little while ago a colleague wrote on her Facebook page,

> "Just found out that the University is expecting me to teach this semester. Last evening was the first I officially hear of this. I got a strange email from a student in the morning asking about the class, so I contacted the school to find out why a student was asking me. The response was, "Didn't you get the contract back in December?" No, I didn't. Then the comment, "See you on Wednesday for class!" Like in TOMORROW??? OMG! That is why I couldn't sleep."

I added to the thread of shocked, sympathetic comments as follows:

> "People don't realize that the definitions of email from the Internet Engineering Task Force Requests for Comments (RFCs) do not include guaranteed delivery. Anyone using email to communicate operationally important information *must* use (a) read-receipts and (b) out-of-band confirmation (e.g., telephone calls) to confirm delivery – and agreement if there's a contract involved!"

The unfortunate incident got me thinking of the wider issue of confirming communications. Supplementary, optional information need not require confirmed delivery, but any operationally-significant information or instruction must have confirmed delivery. Medical offices routinely use an answering message that warns callers not to leave a message if they need emergency help. How would you feel if you had to leave a voice-mail message for an emergency-response team? When the emergency-response operator answers a 999 or 112 call in the United Kingdom or a 911 call in the USA and Canada, every transfer to the appropriate service (fire, ambulance, police) is done with the caller on the line. The caller is immediately transferred to another agent – not told to leave a message.

For technical support and computer-security emergency-response teams, it's essential that the problem-ticket system automatically sends a confirmation message to the client indicating the ticket number for every request for help – a particularly important function when the lines are busy and a client leaves a voice-mail message, or when a client sends a help request through email. With enough exposure to such a policy, clients quickly come to expect the confirmation; if their original request is lost, misdelivered, or ignored, the lack of prompt confirmation from the help desk alerts the client to the likelihood that their message never reached anyone in technical support so they can try again.

When transferring responsibility for a technical-support case from one agent to another, the transferring agent must make person-to-person contact with the agent who will pick up the case; leaving a voice-mail message or sending an email message is not good enough. An interrupted chain of communication will leave a client hanging without support for an indefinite period. An alternative to telephone or in-person contact is instant messaging (IM); an IM request can elicit an immediate response – and failure to respond can prompt further attempts to make contact or perhaps a switch to a different resource person. In any case, the client will never be abandoned because of an interrupted communication attempt.

Since arriving at Norwich University in 2001, I have consistently refused to accept student essays or assignments on paper. For the first few years, I told students to submit term papers and exams using email; however, a few years ago, when our learning platform became available, I switched to using the intranet functions to upload the assignments to a repository for each assignment. It provides a

detailed record of exactly when each student upload his or her file, so there's no ambiguity or uncertainty about whether the student submitted the work on time.

When planning for adjunct faculty staffing, every proposed contract should be confirmed before the contract is sent. My policy would be to make live contact by phone or voice-over IP (VoIP) to ensure that the instructor agrees to teach and accepts the terms of the contract. Then the director of the school or department should send instructions by email to the human resources (HR) group asking for a contract to be sent – and the standard procedure should be that the request is copied to the instructor. The HR group should always send an email confirmation to both the issuing department and to the instructor. If a paper contract is the only format permitted, an HR official should verify that it was received, signed and returned within a reasonable period (say, a week). Lack of response within the stated time would prompt a follow-up call. A checklist would make it easier to ensure that every step of this procedure is completed.

Don't count on luck when interacting on critical, time-sensitive issues: verify email delivery as a matter of course using a different communications channel for positive confirmation of receipt.

16 PROTECTING ORGANIZATIONAL REPUTATION

I first started using email in 1982 at work, when I was a "systems engineer" for Hewlett-Packard Canada. In the early 1980s, E-mail was restricted mostly to businesses and academic users; a few thousand individuals exchanged messages through bulletin board systems (BBSs), and there were various schemes for mail relay among BBSs and value-added networks (VANs) such as Prodigy and CompuServe. Basically, amateurs did not have much exposure to electronic communications.

In contrast, today millions of people have grown up using email, chat rooms and news groups from their childhood or youth, quite apart from businesses and formal organizations. Because of the rapid rise of these high-tech communications media, there has been a rupture in civility. There is a disjunction between the customs of civility and courtesy that were defined for earlier generations in terms of speech, telephone and written communications and the habits of a couple of generations who have developed their own style almost free of guidance from older people.

There is nothing unusual about different modes of communication for different contexts; conversational spoken language, for example, sounds quite different from the formal speech of conferences or the structured writing of an article.

Speech between two long-married people, for example, is highly idiosyncratic. Jean-Paul Sartre once said that a good marriage is like a conversation that never ends, but the conversation becomes quite peculiar after a while. I remember my wife's and my amusement when we heard a tape we accidentally made during a car trip when we must have somehow gotten a recorder going: it sounded completely off the wall ("Is that surprising?" I imagine some of you thinking) with sentence fragments, long companionable pauses, code words (e.g., "Do I have baboons?" "No, you have no baboons."), resumption of topics many minutes later as if there had been no intervening content, and a general lack of any obvious structure.

From a business point of view, however, some of the people most comfortable with electronic communications have developed some bad habits. This series will serve as a guide to standards of appropriate behavior when employees are communicating online. Topic areas include

- Selling products and services
- Spam
- Responsible posting: The prime directive of corporate Net use
- Responsible posting in discussion groups
- Rejecting dishonesty in advertising
- Operational security (OPSEC) in release of company-confidential data

16.1 Selling Products and Services

There is nothing inherently unethical about using the Net for selling products and services, but there are some fundamental problems peculiar to the Net: messages can be

- Immortal
- Modified and become inaccurate
- Forged
- Unwanted.

Messages circulate on the Net without central control. Old copies of documents reside on individual servers and workstations and can be resuscitated years later. Imagine an advertisement for a special price on a company's product; having a client ask for that price two years later might cause problems if conditions have changed. However, from the client's point of view, the message may have arrived from a friend yesterday; even if the supplier explains that the sale is over, the client may be disappointed and perhaps even angry. From a commercial perspective, all communications offering goods and services ought to have a date of origin and an expiration date.

What good is an expiration date if someone alters it before rebroadcasting the message? For that matter, anyone can alter any aspect of a message before sending it back into the Net. The ultimate alteration is forgery: inventing a false message ostensibly from a specific person or organization To avoid embarrassment and possibly litigation based on misleading or libelous documents, one should be able to repudiate such messages. There is no absolute repudiation, but one can build a strong case for repudiating a message if one uses digital signatures on all communications. If thousands of messages have all been signed digitally, then an unsigned message or a message with an invalid digital signatures can reasonably be repudiated.

16.2 Unwanted Messages

There are plenty of ways of marketing products and services electronically without offending anyone, violating standards of civility, or breaking the law. Using the World-Wide Web is one; generating and using legitimate, opt-in email lists is another.

However, there are at least three types of unwanted messages: unsolicited commercial email (UCE), usually called "junk email" and sometimes known as "spam" (much to the horror of Hormel, the trademark owners for SPAM™ luncheon meat); chain-letters; and hoaxes.

Employees who are new to the Net may think naively that sending advertisements to millions of recipients at little or no cost sounds like a great deal. Certainly thousands of gullible nitwits have fallen prey to charlatans selling systems for sending out junk email; many of these novices unthinkingly accept the notion of forging email headers to avoid the consequences of their actions. However, no reputable organization will permit such abusive behavior; junk email puts the organization into bad company, uses the recipients' resources (bandwidth, disk space, time) without permission, and generates outrage from many of the victims. That outrage can take both legal and extra-legal methods.

A notorious case of header forgery came to light in May1997, when Craig Nowak, a college student, chose a return address at random for his first attempt at junk email. Unfortunately for his victim, "flowers.com" was a legitimate business whose owner received 5,000 bounced messages and plenty of abuse for supposedly spamming the world. Fortunately for the anti-spam cause, the enraged florist, Tracy LaQuey Parker, launched a lawsuit for damages and was supported by the Electronic Frontier Foundation and the Texas Internet Service Providers Association. In late September 1997, the plaintiffs won a temporary injunction against the defendant and his ISP preventing him from further use of the appropriated domain name (not that he'd have wanted to, at that point). In November 1997, the defendant was fined $18,910 plus court costs.

A different sort of response occurred in 1994. In the December issue of *Network World* an anonymous writer told the following story. Without knowing that he was violating standards, he posted a message about his company's products on about a dozen USENET groups. Within hours, he was swamped with abusive email, abusive USENET group messages, and – worst of all – his company's 800 number was widely posted in alt.sex groups as if it were a free phone-sex line. The volume of calls (all of which were paid for by the company) by sex-seeking callers not only saturated the company's phone lines, but also annoyed the receptionists to such an extent that one of them resigned and the other forwarded all the 800-line calls to the phone of the employee who started the whole mess. The 800 number had one of those fancy letter combinations and it was all over the company's advertising, business cards,

 and letterhead, so changing the number was not an option; the company simply had to wait for the fuss to die down.

These cases are good enough reason to convince most sensible employees that sending junk email is (shall we put it mildly?) not a good idea for their employers or for their careers.

Page 30 of 34

16.3 Professionalism: The Prime Directive of Corporate Net Use

The most important principle about corporate email that you can teach your network users is that **every communication made using the organization's email system should be considered as equivalent to something written on official letterhead**. Lack of professionalism in such communications can seriously damage the entire organization's reputation and credibility.

We have already looked at spamming – sending unsolicited commercial email. Other forms of unwanted messages include hoaxes and chain letters. Many hoaxes refer to non-existent malicious software; a general policy that makes sense is to explain to all users that they must not broadcast any warnings. Users alarmed by such messages should simply contact their technical support team and let experts investigate (and often debunk) stories of exploding monitors, damaged disk drives and the like. As for chain letters (messages asking people to forward a warning, health information, or a petition to everyone in the recipient's address book), adults ought to know better than to forward such drivel, but at least within the organization, such forwarding can be interdicted by policy.

A simple lack of professionalism is to send or publish correspondence (or worse, articles) with spelling, grammatical or factual errors. Yes, of course no one is perfect, and the occasional blunder is forgivable (I sure hope so, given the errors I have made in print). What I am referring to is slovenly writing: poorly thought-through ideas, poorly expressed. Anyone can use a spell-checker at the very least; even a grammar-checker is better than nothing. But if an employee is involved in public discourse, especially on an important and highly-visible topic, it might be a good idea to have the Public Relations (Marketing, Corporate Communications. . . .) experts check the content and style before launching it into the public sphere.

Another form of unprofessional behavior is "flaming." Many users of email and of the USENET think that making rude remarks about the people with whom they are corresponding is just a normal way of expressing disagreement. But rudeness is unprofessional. It is inappropriate for a professional to use profanity, obscenity, sarcasm, and other demeaning modes of expression. Even more embarrassing is to see correspondents who make *ad hominem* remarks – comments about the personality or personal characteristics of others. "If you had bothered to read what I wrote. . . ." or "You are obviously incapable of understanding my point. . . ." and similar slurs and innuendos demean not only the recipient but also the sender. They can certainly embarrass the sender's employer.

The converse is that as recipients, we need to be tolerant of what may appear to be rudeness. Not everyone has the practice required to write with sensitivity and subtlety, and sometimes people's sentences misrepresent their intentions. There is no cause for a professional to respond to other people's rudeness by descending into the written equivalent of a shouting match, regardless of provocation.

My own practice has been to avoid flaming back when I receive even private communications that cross the rudeness boundary. Over the years, I have occasionally written viciously vitriolic responses to rude people and laughed uproariously at how much fun it is to fight back. Then I have deleted the nastygrams and written back as politely as I can. The professional responses have not necessarily been friendly, but at least they were civil.

Corporate users should be made aware of these principles in policies and in training classes. It might even be fun having users practice responding to rude messages with civil responses as part of the classes.

16.4 Responsible Posting

We have seen in a previous section that posting advertisements in USENET news groups, Facebook, or Twitter (etc.) is a poor idea. Although not all news groups or social media are moderated, there are nonetheless written or unwritten rules about whether advertising is welcome in any given group.

In general, there are some straightforward principles for being a responsible and welcome participant in a news group, social medium, or other discussion forum:

- Lurk before you leap: learn about the specific style in use in the group you intend to join. Do participants use formal or informal language? Do they seem to value pointers to documents produced by companies and other organizations? Is it appropriate to refer to your own products in this particular forum?
- Remember that on the Net, everything you write may be archived and available indefinitely. Keep that in mind at all times before posting anything.
- Don't flame people (as discussed in a previous section).
- Don't troll; that is, don't post deliberately provocative statements or material to irritate or anger other participants into posting angry responses.
- Avoid profanity, ethnic/religious slurs, and other offensive language.
- Stick to the forum/section subject area: don't post materials that are irrelevant to the subject, no matter how interesting you think it ought to be to participants. For example, most people in, say, a Windows technical discussion group would find it offensive to be told about human-rights violations in, say, Lower Slobovia, no matter how important the topic may be in a wider sense.
- Make messages concise. In most groups, netiquette proscribes quoting an entire message; generally it's enough to quote just enough of a text to make it clear how your response is germane.
- Respect copyright laws: don't publish someone's comments elsewhere without asking for and receiving permission. Don't post screenshots of other people's intellectual property without permission. Links are fine, though.

16.5 Honesty: No Covert Ads or Shills

In addition to the general rules on civil collaboration in discussion groups and mailing lists, vendor staff should understand that only honesty is acceptable in selling products. It is unacceptable to post forum messages that are covert advertisements. Responses should be focused on the issue at hand and should be as helpful as possible. Forums, newsgroups may have strict standards and there may be negative responses to introduction of your company name and product without clear benefits to recipients. Repeated marketing hyperbole in technical forum repels potential customers. Indeed, even subtle propaganda will be punished: beware of posting superficially-objective responses that are slanted: misleading information will inevitably be punished by public exposure, humiliation of the guilty, and embarrassment of the employers.

Much worse than propaganda from an identified employee of a company is propaganda in the guise of disinterested comment. Company policy should make it clear that employees who are posting information that is relevant to company interests should clearly identify themselves as employees. Commenting on competitive products or services or praising one's own without clearly identifying oneself. Such shills are highly objectionable, and group members will often express their disapproval in the strongest terms. Shills may be locked out of controlled-access groups, both individuals and employers may receive torrents of abuse, and the effects may last for a long time.

Conversely, it is appropriate to post a disclaimer when appropriate to indicate genuine disinterest; e.g., "Neither the authors nor their employers have any financial interest in the companies, products and services mentioned in this communication."

* * *

In 2011, one of my students, Todd Renner, published a series about "sock puppets" and "astroturfing," which are terms for automated, misleading, and fraudulent posting of praise for an organization or abuse of a competitor. See the following:

- Online Reputation Management: Manipulating Search Engines
  < http://www.mekabay.com/nwss/909_orm_manipulating_search_engines_(renner).pdf >
- Online Reputation Management: Dishonest Methods
  < http://www.mekabay.com/nwss/910_orm_dishonest_methods_(renner).pdf >
- Online Reputation Management: The BP Case
  < http://www.mekabay.com/nwss/911_orm_bp_case_(renner).pdf >

16.6 OPSEC: Don't Talk to Strangers

There's a funny thing about becoming an active member of a discussion group – whether in real-space or in cyberspace. The longer you participate, the closer you feel to the regulars. There's a sense of camaraderie, of belonging to a group of interesting people; indeed, in some real and electronic groups, the regulars act like a regular clique. Like the snotty brats in high-school cliques, these folks treat newcomers with disdain and assume a position of superiority that can be truly offensive.

However, that same sense of camaraderie, even when it is expressed positively and not through putting down others, may fool employees into forgetting that they don't necessarily know with whom they are corresponding. Furthermore, they don't know who is lurking (reading the exchanges without contributing). The audience may very well include people from direct competitors, and there is nothing illegal about using information that is posted openly in a public forum.

Employees should not post intimate details of a particular project, a new product version, plans for expansion in a new geographical area, their employer's marketing strategy or inside information that could violate Securities and Exchange prohibitions on revealing insider information that could affect share prices. Appropriate use policies should make it clear to everyone that by definition, confidential information may not be disseminated outside the organization. Only the Public Relations or Corporate Communications / Marketing departments would normally be authorized to decide how and what to post publicly.

The principle of discretion applies equally well to criticisms of the employer, partners, suppliers, or individuals. It is foolish to think that broadcasting internal grumblings about an employer will be ignored by management. Such public criticisms can severely damage the organization. Now, if the organization is breaking the law, employees can report the crimes to law enforcement or regulatory authorities; however, posting details in public may make it difficult or impossible for investigators to gather information that will be usable for prosecution. Employees who have resigned or who are fired might also want to check the terms of their contracts; some employment contracts impose a gag on criticism even after an employee has left the employ of an organization. When in doubt, consult an attorney with experience in employment law and litigation.

One last note: employees should remember that most of what is posted on the USENET and today's World Wide Web is archived and can be available to prospective employers years later. If employees fail to protect the interests of one employer, what would convince a new employer that their discretion would be any greater in the future?

ℭ℘℘