

# Using E-mail Safely and Well

Version 4 (March 2011)

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

## Contents

Using E-mail Safely and Well Version 4 (March 2011) .....	1
1 FIRST E-IMPRESSIONS.....	2
2 DISCRETION IN E-MAIL CRITICISM.....	3
3 HTML-FORMATTED E-MAIL DOESN'T WORK RELIABLY .....	5
4 CC + REPLY ALL = TROUBLE:.....	7
5 BCC PREVENTS E-MAIL NUISANCES .....	8
6 BURYING YOUR E-MAIL MESSAGE.....	10
7 MISLEADING SUBJECT LINES .....	12
8 E-MAIL DISCLAIMER STIMULATES EXPLETIVES .....	13
9 FORWARDING CORPORATE E-MAIL.....	15
10 E-MAIL SUBJECT LINES EXPLOITED BY WORMS.....	17
11 INTERNET E-MAIL AND THE FIREWALL .....	20
11.1 Management Implications of External Access.....	20
11.2 E-mail Access to FTP.....	20
11.3 Denial of Service.....	20
12 ORGANIZATIONAL E-MAIL ADDRESSES.....	22
13 THE KEEPER OF THE LISTS .....	23

Download this file from

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

# Using E-mail Safely and Well

---

## 1 FIRST E-IMPRESSIONS

When you receive an e-mail 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 e-mail 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 e-mail 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 e-mail 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 slob. Questionnaires 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 e-mail, 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 e-mail, first impressions really do count. Professionals should carefully review e-mail messages for acceptable writing, including word-choice, punctuation, capitalization, and spelling.

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

---

# Using E-mail Safely and Well

---

## 2 DISCRETION IN E-MAIL CRITICISM

In this series on discretion, I started with general guidelines about expressing opinions when on the job and representing one's employer < <http://www.networkworld.com/newsletters/sec/2011/031411sec1.html> > and then moved on to special restrictions on people wearing military and other uniforms < <http://www.networkworld.com/newsletters/sec/2011/031411sec2.html> >. Today I want to touch on awareness about e-mail protocol.

In a paper entitled, "Using E-mail Safely and Well (v3)" < <http://www.mekabay.com/infosecmgmt/emailsec.pdf> > I cover some fundamentals of secure use of e-mail such as proper choice of subject line, the use of CC and BCC, and so on. However, there's another topic I'll add to the paper: discretion in sending off-the-cuff critical comments to someone via corporate e-mail.

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 e-mail: 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 e-mail 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 e-mail. 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](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 analyses 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

## Using E-mail Safely and Well

---

- 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?”

In my experience, many people don’t edit their e-mail messages at all before sending them; some don’t even check their spelling. Under those circumstances, an e-mail 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 e-mail, 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 e-mail?
- 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 e-mail?
- 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?

In my e-mail client, I have a 30-minute send-cycle; unless I cause an immediate SEND, my e-mail 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.

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

### 3 HTML-FORMATTED E-MAIL 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 e-mail messages (as distinct from attachments) *does not guarantee* preservation of the exact appearance of the source material.

Attractive, well-formatted e-mail 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 e-mail 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 e-mail for security reasons. All such formatted e-mail 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 e-mail 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 DOC files, WordPerfect WPD files, or Rich Text Format (RTF) 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).

## Using E-mail Safely and Well

---

So if the exact appearance of a message you are sending via e-mail is critically important to you, you can send the content *and* its format in a way that is (largely) platform independent: 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 Adobe Acrobat installed so that you can either "print" to an Acrobat driver to create the PDF files or even just click a toolbar button to do so from within your word processor. 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 XL 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 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.

### 5 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.

## Using E-mail Safely and Well

---

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.

### 6 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](mailto: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](mailto: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:

- **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](mailto:bob123@genericemail.net).
- **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.
- **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.
- **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

## Using E-mail Safely and Well

---

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).

### 7 MISLEADING SUBJECT LINES

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 e-mail: 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 e-mail labeled, “Birthday party 12 May.”

Not all e-mail messages are created equal; some are destined for the trash heap, if not of history, at least of the e-mail system. That decision is sometimes made automatically as a function of the subject line. For example, I usually flag e-mail 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 line of these messages to my filter, my e-mail 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 e-mail message whose subject line implies otherwise. For example suppose an e-mail 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 line as descriptive as possible without turning it into a paragraph. Some e-mail systems truncate subject lines in the display of messages that a users sees; it makes sense to put keywords at the front of the subject. I encourage my staff to use prefixes such as “MSIA:” or “SGS:” to help organize their messages. Using standard formats in subject lines 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 line, where c represents the class (e.g., 7 for students starting in September 2005) and s represents the seminar number.

## Using E-mail Safely and Well

---

### 8 E-MAIL DISCLAIMER STIMULATES EXPLETIVES

One year, I received a 30-word e-mail message from a very nice reader in Britain and noticed that his e-mail 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

## Using E-mail Safely and Well

---

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 e-mail 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 e-mail message, you can use a slightly modified British expression in your response: “UNSTUFF IT!”

### 9 FORWARDING CORPORATE 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

## Using E-mail Safely and Well

---

their computers so that the received, decrypted data are not susceptible to discover if someone steals their laptop or home computer.

# Using E-mail Safely and Well

---

## 10 E-MAIL SUBJECT LINES EXPLOITED BY WORMS

One 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 HTML-enabled e-mail, 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
-RuADZVmR31168x591fL6
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>
-RuADZVmR31168x591fL6
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: wangj1@dsp.ac.cn
Received: from dsp-ns.dsp.ac.cn ([159.226.219.1]) by
siaaglaa.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
siaaglaa.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
```

## Using E-mail Safely and Well

---

```
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=RuADZVmR31168x591fL6
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:

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

## Using E-mail Safely and Well

---

And the ever-popular general principles,

- Choose antivirus products that can update themselves automatically and make sure they do so.
- Enable automatic scanning on file open and file save.
- Scan your entire system regularly (I configured BitDefender to scan all disks at one in the morning every Saturday night).

## **11 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.

### **11.1 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.

### **11.2 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.

### **11.3 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

## Using E-mail Safely and Well

---

disk storage. Useless e-mail should be purged periodically as a normal function of system house-keeping.

### 12 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](mailto: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.

### 13 THE KEEPER OF THE LISTS

The School of Graduate Studies at Norwich University is large enough that there is significant turnover among the staff. Until recently we were 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 SGS must maintain to be able to distribute e-mail to appropriate groups. I remember one time, I noticed that on all-SGS 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 have 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 can 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 is an utter kludge and I don't like it because we are putting our faith for continued production application in a free resource completely out of our control].
- IT can install widely available list-server software to allow the KL to create and maintain specific lists; e.g. SGS-ALL, SGS-DIRECTORS, MSIA-STAFF, MSIA-INSTRUCTORS, etc. that all of us can use as addresses for e-mail.
- IT can switch all SGS users to any e-mail client that supports exportable mailing lists (e.g., Outlook 2003 because we support the rest of Office 2003). The KL can maintain and distribute updated corporate distribution lists. However, this solution still requires manual intervention by users: everyone has to replace their old list by the new list.
- IT can implement Microsoft Exchange Server, switch all SGS users to Outlook 2003 and define corporate distribution lists maintained by the KL. All users will automatically access the one and only distribution list for each group without manual intervention.

