By Gregory A. Jackson

Yes, You Can Trust Your E-Mail

A traveling dean needs some sensitive data immediately. Reading tables over the phone won't work. A messenger is slow and expensive. You could fax, but hey, the data are on your computer already, so you do the obvious: e-mail.

Are you right to trust e-mail for this private, sensitive communication? Some say "no": computers aren't secure; hackers can penetrate mail servers; and strangers on the Internet can read e-mail in passing. On the other hand, in practice each of these risks is small—certainly no greater than those in campus mail—or can be minimized, as I will explain below.

An e-mail message's journey typically has seven stages. You compose it on (A) your computer. Next comes (B) transmission to (C) an outgoing mail server, from there (D) transmission to (E) the recipient's incoming mail server, and finally (F) transmission to (G) the recipient's computer.

Internet lore to the contrary, typically the greatest risk of unintended disclosure lies neither in transmission (B, D, F) nor servers (C, E). If I, as a bad guy, want to read e-mail between you and the dean, my last resorts are to intercept it or to crack servers: my first choice is to steal your computer (A) or the dean's (G). The principal security risk is thus the same for both e-mail and paper mail: the accessibility of the sender's and recipient's file copies.

Can't Other People Read E-Mail on My Computer?

If you lock up your computer as you do paper files, you're probably okay. This is the simplest e-mail security measure and the one most frequently overlooked. Too often I watch colleagues or their assistants carefully lock file cabinets and then leave undefended computers in the open. Instead, they and you should secure desktop computers by keeping them behind locked doors or by installing and using access controls. At the very least, the computer should require a password—a password neither shared nor written down—before it can be used.

Even on a secure computer, delete mail you don't need, and remember to "empty trash," "purge deleted messages from server," or take whatever other steps are required to actually get rid of deleted messages. This is the only reliable defense against subpoenas and other, increasingly common legal mechanisms for forcing disclosure. Trash-it strategies conflict with good records-management policies, however, so some discussion with your records manager or institutional archivist is worthwhile.

Encrypt sensitive messages (or other documents) that you must keep. Unfortunately, encryption requires special tools and some training, and it introduces a risk of its own: if you lose the decryption key, the message is useless. For this reason, universities and other institutions increasingly require that copies of decryption keys be held centrally—in "key escrow"—so that business information can always be retrieved. Unfortunately, escrowed keys are also subject to subpoena.

Can't Someone Get Copies of My E-Mail Kept in the System?

Generally, no. Outgoing-mail servers (C) keep logs of messages transmitted, but these include only header information (who to, who from, subject). They keep no record of the messages themselves. Incoming-mail servers (E) usually do the same. But there are two important exceptions. First, until the recipient retrieves a message from an incoming-mail server, the full text is on the server. If users intentionally leave mail on the server after they've retrieved it, then messages remain on the server even longer. Someone with the right access privileges can retrieve these "spooled" messages. This is why incoming-mail servers should be kept very secure, why they should not share hardware with other services, why access to them should be limited to highly trusted network staff, and why it is important to have clear policies and procedures for disclosing information from mail spools.

The second exception concerns storage. Well-managed computers get regular backups, meaning that everything on them gets copied to a different location. On some computers, "private" files, including e-mail files, are actually stored on shared or central file systems. When backups or remote-file systems include mail files—be they the sender's, the recipient's, or the server's—messages are only as secure as the remote storage. As you may recall, Oliver North and Bill Gates both learned this lesson too late. It is one of many reasons why centrally managed, network-based backup and remote-file systems can be preferable to widely distributed, locally managed ones: the former generally have well-defined and enforced security policies and procedures.

Can't Strangers on the Internet Read My E-Mail in Passing?

Again, no, with one exception. When your mail travels over the Internet (B, D, F), it's usually handled according to a set of rules and procedures called Transmission Control Protocol (TCP). TCP breaks your message into a series of small packets containing address information, reassembly information, and chunks of message. As those packets traverse the Internet, the servers that handle them use Internet Protocol (IP) to determine the best route and therefore which server should handle each packet next. Although the packets constituting a message usually travel the same route one after another, they rarely do so in unbroken series, since other packets are traveling the same route. Sometimes one message's packets actually travel various routes if bottlenecks develop. When a message's packets arrive at their destination (C, E, or G), they get reassembled so that the server or the recipient's computer can handle them as messages rather than packets.

The problems for bad guys trying to intercept your mail are obvious: they must position themselves at a time and place where your packets will be in transit, they must gain access to the TCP/IP traffic stream, and they must pluck your message's separate packets out of that stream. Each of these presents forbidding obstacles. First, exact timing and routing are hard to predict. Second, Internet carriers protect their conduits, physically and technically, so access is difficult. Third, given today's network speeds, even a modest attempt to capture a TCP/IP stream (called "sniffing") produces so much data that bad guys need very substantial computing power and/or data storage to handle it. According to a recent *New Yorker* article, even the National Security Agency lacks the capability to do this effectively.

Bad guys might succeed more easily, however, if they could use a computer on the same subnet as your computer (or your correspondent's). Local subnets (the collection of connections from your computer and others near it to a closet nearby, where the whole subnet is connected to the campus backbone) often handle traffic by Ethernet routing. Routed subnets work much the same way that a sushi restaurant I saw in Palo Alto gets maki to customers: packets simply float around in a circle on the subnet, and each computer on the local network grabs the packets destined for it.

The risk is obvious. Someone on a subnet managed this way can retrieve packets belonging to someone else on the same local network. It's one of the major reasons network-security folks worry so much about unauthorized access even to "personal" computers. One carelessly managed machine can compromise all the traffic on a routed subnet. Things improve if "switching" replaces "routing." On a switched network, packets go only to and from the backbone portal in the closet, rather than float around visibly to others. As campuses move to high-performance networking, for example to participate in Internet2, they typically replace routed with switched networks. Therefore, on these campuses, local-network sniffing is becoming much less of a problem. Unfortunately, small, locally managed subnets remain under departmental control on many campuses. Often these do not operate in ways that promote e-mail security.

So How Do I Ensure That Private E-Mail Remains Private?

First, tell everyone—e-mail users, e-mail system operators, and network architects alike—about the reasonable measures that they and their correspondents should take. Second, encourage everyone to exercise the same care with e-mail that they do with other conversations. Third, encourage IT practices and architectures that improve rather than degrade privacy. Fourth, begin thinking about encryption. If a message is encrypted, then many of the risks I listed above—interception, unauthorized retrieval from servers, even stolen computers—become much less important.

Most of all, the continuing trustworthiness of e-mail depends on the continuing application of common sense—by you, by your e-mail recipients, and by your IT people. Private e-mail generally stays private, especially in transit. It arrives promptly and in useful form. It is trustworthy. You were right.

Gregory A. Jackson is Chief Information Officer at the University of Chicago (e-mail: gjackson@uchicago.edu).