IT Policy:
E-mail Threats Are No Longer a Laughing Matter in Virginia

by   Chip German
        Director, Policy and Planning
        Office of Information Technologies
        University of Virginia

Kids say the darndest things. So do adults. Sometimes adults use hostile words playfully—they may say "I'm gonna wring your neck" or "You'd better clean that room up right now or I'm gonna whup you upside your head," but they usually don't mean those things literally (do they?).

The differences between words and the meaning intended by the person who speaks them have been perplexing humans since they developed the capacity to be perplexed. It won't be a surprise to you to hear that electronic communications carry their own special issues in this regard. But it may surprise you to know that the Virginia General Assembly recently upped the ante on the possible consequences of using words in e-mail that don't exactly match your real intent.

In its 1998 session, the General Assembly amended the Code of Virginia (§ 18.2-60) to include—among the threatening communications punishable as a Class 6 felony—"electronically transmitted communication producing a visual or electronic message." This means that if you send an e-mail message that threatens to kill or do bodily harm to the recipient or a member of his or her family, you may have committed a felony in Virginia. This particular variety of felony can get you up to five years in jail and up to $2,500 in fines.

Whoa, you think—most times that we see e-mailed threats, they are jokes. How can we be sure? Let me start this discussion by reminding you that I am not a lawyer. If you have any question about the definition of an electronically communicated threat—or whether your own language constitutes one—consult someone who is.

How can we be sure an electronically communicated threat is a joke? We can't see the expression or hear the exact tone used by the person who generated the language, unless the author has been so obvious as to use a laughter "emoticon" to indicate what the proper response should be. Usually, we don't have such cues. Electronic communications often leave out the elements that help the recipient of a spoken threat assess how serious it is. So the person receiving an electronically communicated threat is more likely to be worried about it than someone with a full range of visual and auditory communication cues. Add to that likelihood the other unnerving and frequently present condition: it is relatively easy for the person generating an electronically communicated threat to hide his or her identity. Together, those conditions probably lead more recipients of electronically communicated threats to report them to authorities than people who are threatened in person. That's where computing-system staff enter the picture.

Those of us who work for computing organizations are often the hapless folks who receive reports of e-mailed threats. We are usually in a worse position than the recipient to evaluate whether or not a threat is serious, although sometimes we can provide valuable information that can help others in judging that question.

For example, at the University of Virginia, it is against policy for a user of our computer systems to hide his or her identity in order to avoid responsibility for his or her actions. If a person receives an anonymous threat, we may be able to discover which account sent the message (and with it, the apparent identity of the sender) with the help of system logs and similar information sources. Unfortunately, the most common defense used by account holders when confronted about such matters is that the security of their accounts had been compromised by unknown parties, hence the use of the word "apparent."

There are many more details about how we will handle such complaints than will be of general interest, so I won't discuss them here. The most important message for everyone to get is that e-mailed threats are now much more likely to be reported to the police department than they would have been in the past.

Internet users in general—and our students in particular—have grown accustomed to some tolerance or at least skepticism about the seriousness of threatening language in e-mail and other forms of electronic communication, notably in such forums as the Usenet newsgroup alt.flame. "Flaming" is an entertaining hobby for some of them. But, all members of the computer-using community at our university—and all who communicate with anyone in Virginia—now must recognize that using such language outside an obvious and apparent context of harmless fun may subject them to criminal investigation. E-mailed threats are no longer a laughing matter in Virginia.

E-mail Threats Are No Longer a Laughing Matter in Virginia: Handling Complaints at U.Va.

by   Chip German
       Director, Policy and Planning
       Office of Information Technologies
       University of Virginia

In the past, if both persons involved were students, we provided information about the communication to professionals in the student-affairs division so they could determine whether a serious threat existed. In part, we took this course of action because electronic communication is usually a communication crossing some distance in both time and physical location. So we believed that most electronically communicated threats to kill or injure—without what "Black's Law Dictionary" in the definition of the term "assault" calls "an apparent present ability so to do"—probably weren't acts requiring that we directly and immediately notify our police department, as opposed to

the Division of Student Affairs. Because of this practice, Student Affairs has in recent years uncovered many joke-threats and has intervened effectively in the much smaller number that had some real hostility and potential for violence behind them.

But the new language in the Code of Virginia explicitly adds such mechanisms as e-mail to the ways felonious threats can be communicated, and there is no language requiring an "apparent present ability" to make it against the law. The law dictionary does indicate, however, that, for a threat to be prosecuted, it must be a "true threat," which is different from "words uttered as mere political argument, idle talk, or jest."

The entity that would investigate such threats is most often the University of Virginia Police Department, and prosecutions related to e-mailed threats sent from or received at the University of Virginia would often originate in the offices of one of the area's Commonwealth's Attorneys. Because of this change in the language of the law, the University's computing staff will immediately report any e-mailed or otherwise electronically communicated threat that comes to our attention to the police department, if we have been unable to determine rapidly and definitively that it represents political argument, idle talk, or a joke.

My experience tells me that we'll have to turn over to the police the vast majority of the threats about which we receive complaints. The volume of such complaints is small at the moment—it peaks at two or three a month. But, as we have seen before, when our user population becomes more aware of what can be done about something, reports increase rapidly. We will not be surprised to see the number of complaints rise as more people become familiar with the change in the language of the law. And, in all cases, our "abuse" investigation system will ensure that the student-affairs division is aware of complaints about e-mailed threats as before. The primary change will be the early and direct involvement of our police department in these complaints.