## Beacon Hill Byline

## "Deleting E-mail scams"

This week the Byline is taking a break from state political issues to provide a public service to readers. To warn people away from responding to a growing number of email messages offering the recipient a chance to share millions of dollars with the sender. Do not respond to such messages. Delete the messages immediately from your computer!

A sampling of the messages from my own e-mail account includes appeals purporting to be from Nigeria, Congo and the Netherlands. The messages say I have been selected to help the sender get millions of dollars that are tied up because of political intrigue and praise my integrity and discretion, although I am addressed as "Dear Friend" or "Sir/Madam." In return for that help, the authors will give me 20% to 25% of the \$10 to \$20 million, according to the scam.

One letter talks of frozen bank accounts in Africa that can be released to me if pretend to be next of kin to an accident victim. A second has so much faith in me that he invites me to put together an investment portfolio worth millions of dollars. Still others ask me to help a deposed leader remove millions of dollars from a Dutch bank.

The scams are the 21<sup>st</sup> century's version of the old scheme in which the perpetrator approaches an individual on the street and offers to share a windfall if that person puts up "good faith" money of his own. Anyone who responds to the e-mail contact will have to prove suitability for the "partnership" by showing that I have money in the bank.

At the request of a constituent who had received a similar letter by mail with a Greek postmark, I consulted with the Massachusetts Attorney General. His office responded that such letters are fake, but law enforcement is unable to stop such solicitations that originate outside of the country.

A stronger warning came from the Massachusetts Bankers Association. Some customers have been tempted by the promise of easy money and responded to the e-mail. They are then asked for personal identification and at some point the victims provide their bank account numbers to the perpetrator. Though they wait for money to be wired into their account, money is only transferred out, both out of the bank and out of the country. According to the Association, one western Massachusetts customer lost \$20,000 from her bank account before her banker identified the scam and intervened to help her.

Victims, even after they discover they have been cheated, may be reluctant to report the crime because the original solicitation often implies that they are engaged in a certain amount of illegal collusion. If you believe you may have responded to an e-mail that makes you vulnerable to having money removed from your bank account, contact your bank immediately. If you have actually lost money from such a scam, contact the U.S. Secret Service.

These guidelines will serve you well in defending against this and other financial frauds.

Never provide bank account, credit card or Social Security information by phone or computer unless you have initiated the contact.

If a proposal sounds too good to be true, be assured that it is too good to be true.

Please share this information with friends and relatives, especially with anyone who may by nature be vulnerable to approach from a stranger.