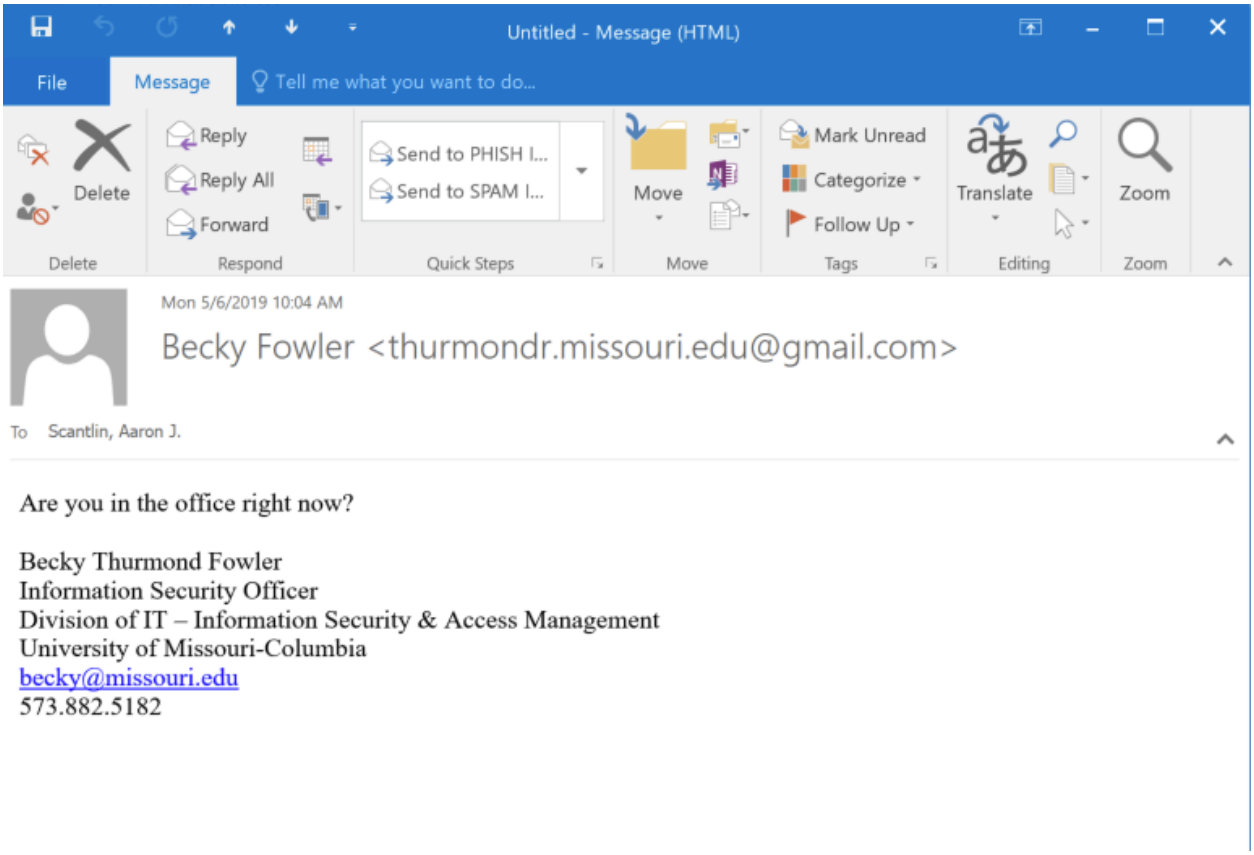
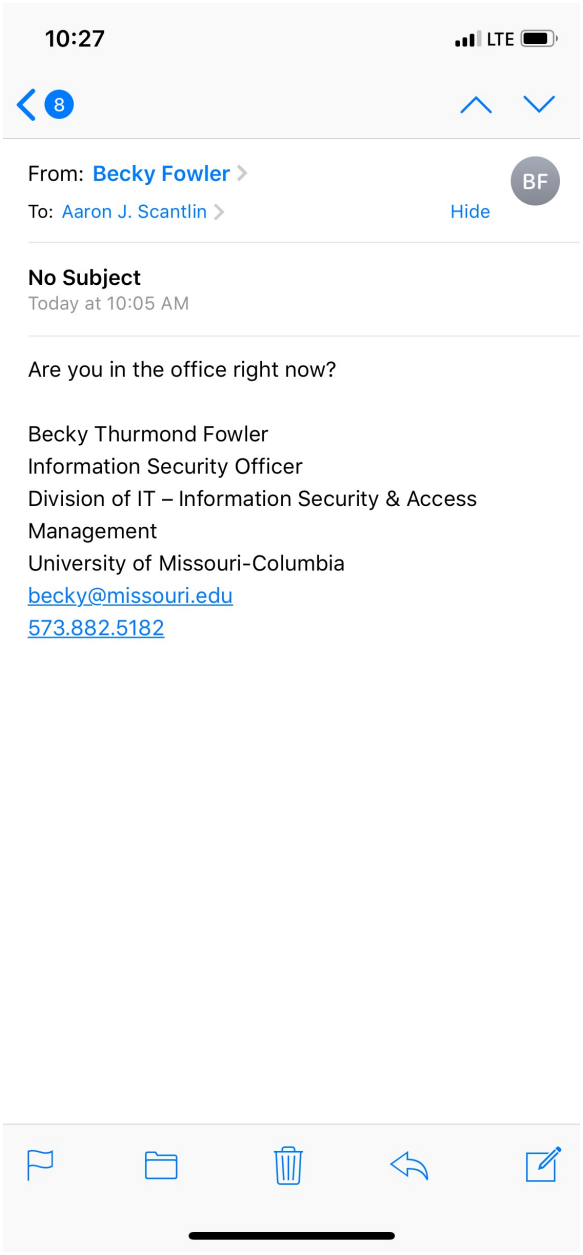
In recent weeks, ISAM has seen a sharp increase in the number of so-called "display name spoofing" e-mails. Display name spoofing is the name given to a phishing technique that tries to convince the recipient of an e-mail that the e-mail was sent from a trusted sender (usually a co-worker) even though the attacker doesn't have direct access to the trusted sender's account. This technique is especially effective against victims using a mobile device to send and receive e-mail since mobile e-mail clients display less information about the sender than desktop clients.

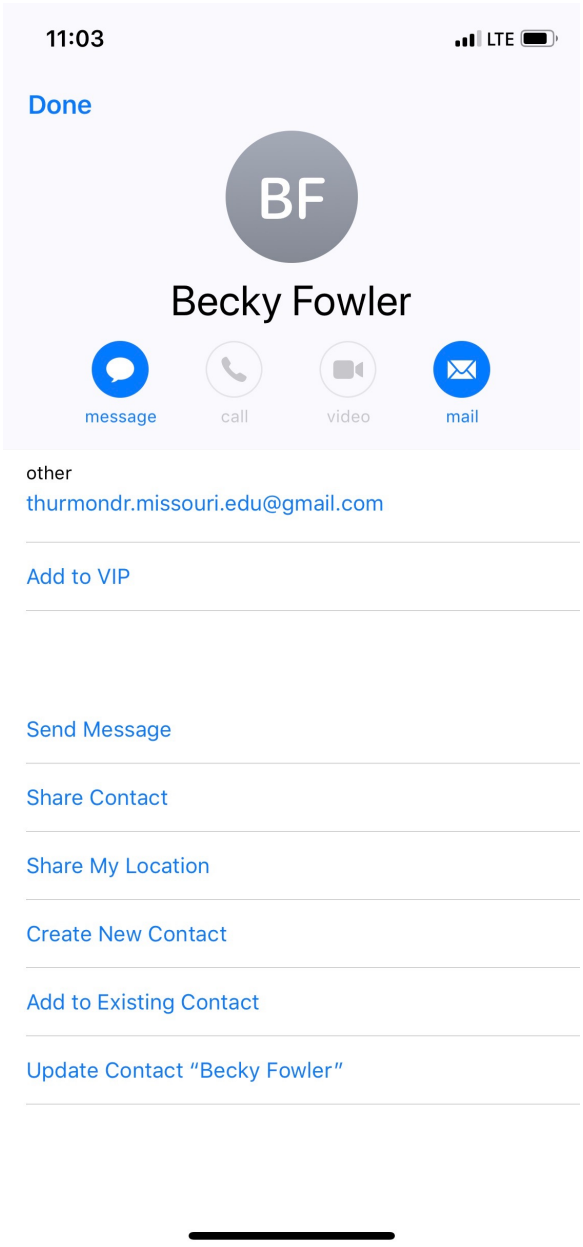
Of course, they say a picture is worth a thousand words, so let's proceed with a concrete example of how someone might try and impersonate the MU ISO, Becky Fowler. In less than one minute, I was able to sign up for a free e-mail account (I used Gmail, but there are literally dozens of providers out there) and send a message to my personal account as seen in the screenshot below:



On a desktop client, this is a pretty easy-to-spot phish; the gmail.com address is a dead giveaway.

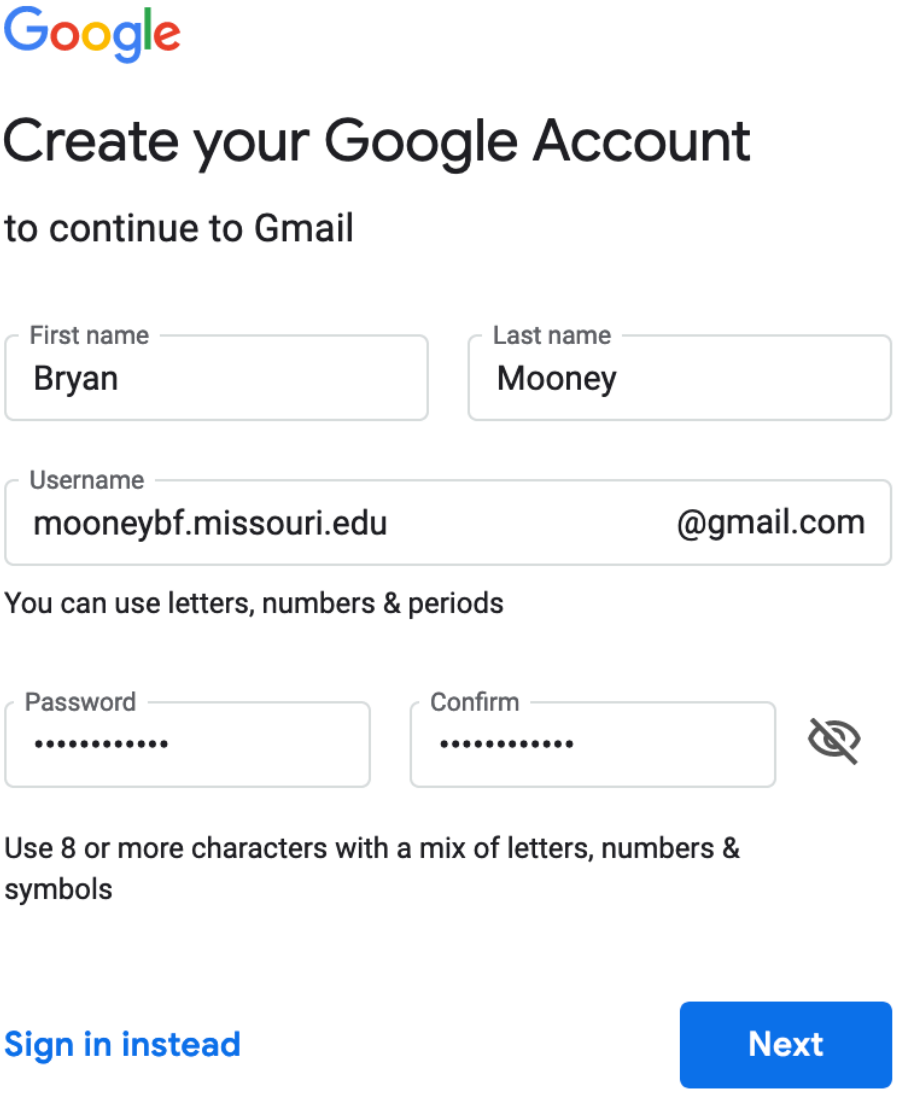
However, let's see how this same e-mail looks on Mail for iOS, a common user client:





Oof… now that is **much** more convincing! However, in Mail for iOS, if you train your users to tap on the "From" name seen in the screenshot on the left, they'll see the information displayed on the screenshot shown on the right. These steps may differ slightly between individual mobile e-mail clients, but the basic steps to sanity check the sender should be the same.

As you can see below, this process can be done for anyone provided the attacker knows someone's first and last name and SSO; this information is publicly available for many department heads through their College's webpages.



Since this is such an easy attack to accomplish, ISAM is asking all members of Distributed IT to take a moment to understand this attack, how it can be leveraged against your users, and to communicate these risks to your users; remember, anyone can send any e-mail they're even slightly suspicious about to abuse@missouri.edu and we'll be happy to check it out!