

Mysterious email, possible social engineering, whatever it was, it didn't work

 devblogs.microsoft.com/oldnewthing/20131210-00

December 10, 2013



Raymond Chen

A colleague of mine got a strange piece of email. It went something like this, although I've substituted a fictitious nation and fictitious company name to protect the guilty(?).

Subject: St. George's Island Embassy Trade Mission: Meeting request on behalf of Contoso Corporation

Dear <name>,

I am contacting you following the advice of <senior executive>, CTO of Microsoft Pangaea.

The St. George's Island Embassy Trade Mission is currently assisting a local company, Contoso. Contoso would like to present <technology> to Microsoft. Details are in the attached document.

Would you accept a conference call with the CEO of Contoso, at a time at your convenience?

Looking forward to a fruitful collaboration,

Sir Humphrey Appleby,
Director, St. George's Island Embassy Trade Mission

My colleague has no connection with St. George's Island, nor had he ever met the named senior executive (or anybody else from the Pangaea division), and he asked, "Is anybody else getting messages like this?" I suggested that they might be trying some social engineering: "Send an email to an employee saying that a senior executive told us to contact them. They will do whatever we ask because they think we are operating under the instructions of the CTO."

This sounded plausible, so my colleague contacted said senior executive, who replied, "I had invited Contoso to participate at a large event we held on St. George's Island last year, but just as you don't know me, I don't know you either. This is definitely suspicious. Thanks for taking the time to send me this warning."

Raymond Chen

Follow

