#yourbossdoesnotneedgiftcards

From:
XXX.subdomain.berkeley.edu@gmail.com
Subject: vendor payment
To: xxxxx@berkeley.edu

Are you around?

<Name Removed>
University of California, Berkeley

From: XXX.subdomain.berkeley.edu
Subject: Quick question
To: xxxxx@berkeley.edu

I'm in a meeting and need help getting some Amazon Gift Cards

<Name Removed>
University of California, Berkeley

Notice that the attacker is sending the email from a Gmail account instead of a berkeley.edu address, even though they claim to be associated with the university.

These email scams rely on social engineering tactics to engage in conversation with victims. The attackers leverage authority and urgency in their requests and will frequently impersonate high-level executives, Deans, or Chairs of departments. These attacks work because they are a simple, quick way to get money from their targeted victims, especially when the email is impersonating someone in the organization.

Look to make sure the email address is correct. In Gmail hover your mouse over the sender name for the email to display. On a mobile phone or a touchscreen, press and hold the link (don't tap!) to reveal the actual URL. Follow-up with the individual directly in a separate email or call/text to confirm.

If you discover the email is a phish, report it! http://security.berkeley.edu/phishing/report