**Step 1. Are you busy?** You receive an e-mail *appearing to be* from someone in your organization in a position of authority. It may be the president, a VP, your Dean or department head. The message simply says something along the lines of '*Are you busy?*', "Hi," or "Urgent".

**Step 2. The follow-up exchange**. Focused on the belief that this person is requesting your help, you reply offering your assistance. To which the sender goes on to say something like, "*I'm in a meeting right now and that's why I'm contacting you through here. I should have call you, but phones are not allowed to be use during the meeting. I don't know when the meeting will be rounding up, and I want you to help me out on something very important right away.*"

**Step 3. Buy something, I'll Reimburse you.** You are still engaged and determined to help. You have missed the warning flags of the non-FSU e-mail address, the poor spelling/grammar, then the imposter makes this request, "*i need you to help me get an [Apple iTunes, Google Play, or other gift card] from the store, i will REIMBURSE you. I need to send it to [nephew, donor, VIP, etc.] and it is very important cause i'm still in a meeting and i need to get it sent Asap.*"

**Step 4. Scratch-and-Send.** If you are still engaged, here is where the money is lost. The imposter will ask you to do something like this, "*I want you to procure [qty 5, 10, 15] of $100 worth [Apple iTunes, GooglePlay, other gift card]. After purchase, You should scratch-off the back code and email clear pictures of all the codes because I am sending them out to the [nephew, donor, VIP, etc.] via email. Make use of the credit card. Kindly keep the physical card after emailing the pictures to me for proper documentation."*

**Step 5. I wish I hadn't done that.** If you allow yourself to get to step 5, there is little chance of getting your money back.

The best protection against this scam is common sense and to apply these three steps: **STOP. THINK. CONNECT**.

1. **STOP – Verify the senders address */* do not respond to the scammer**. In every case, the scammer was using a non-FSU.edu e-mail account with a look-a-like display

name for someone on campus. (E.g. 'Philip Kraemer' pkraemer@gmail.com, or pkraemer@fsu.edu ). If you are just quickly looking at the display name, you may think this is a message from a legitimate source. It is not.

2. **THINK – Is there something unusual about this request?** Verify the senders e-mail address. Why are they asking me to do this? Why didn't they simply ask their administrative assistant or their significant other?

3. **CONNECT – Reach out to a trusted colleague.** Ask for a second opinion, contact the **IT Service Desk** or report the message abuse@fsu.edu . Messages reported to this address will be reviewed, and someone will follow-up with you if any additional action is needed. Where appropriate, the scammer e-mail address will also be blocked on the campus e-mail servers. You may find that someone else may have received this very same 'important' request.