From: Rosen, Lee
Subject: recent email scam targeting medical students
Date: Friday, January 21, 2022 4:41:02 PM
Attachments: image001.png

Hello Students. Below is information on a recent email scam targeting medical students. Please reach out to me or Drs. Kulaga, McNamara, or DeAngelis if you have any questions or concerns.

Thanks to our excellent Information Services team for crafting this message, which you should all take a minute to read:

Recently a number of students received emails from an address that appeared to be that of a faculty member offering them a research opportunity. This was, unfortunately, a scam that could have cost those students thousands of dollars. The police have been notified.

Email is an important communication tool that is used heavily in our academic, professional and personal lives. Unfortunately, it is also a way for malicious activities to impact our lives. Phishing scams typically come as an email, look like they are from a source that you may trust and/or try to scare/intimidate you into doing something or giving away information that you normally would keep to yourself. Scammers rely on people acting quickly on electronic communications and adhering to institutional hierarchies.

Occasionally, a faculty member's name (or someone else you may be familiar with) may be displayed as the sender while the address next to it is not an institutional email address. Sometimes it may look like the name and the address is from our institution. Using various tricks to make an email believable is a common way for scammers to get your attention – they pretend to be someone in your organization, quite likely your boss or trusted colleague - and ask you a simple question to get you to respond. Then they will lead you down a path that seems believable. Often it is something like "can you run out and by me gift cards/equipment/something and I will reimburse you later." They may ask you to divulge personal information that may be used in identity theft.

General guidelines to protect yourself are to not click on email links in emails you weren't expecting, double check the sender (is it someone you know/trust? can you double-check), if it sounds too good to be true, it is. Also remember that anyone who has a legitimate opportunity for you would not take it away because you took time to talk to a trusted mentor, faculty member or other school resource.

If an email looks suspicious, check it out. Don't act on it.

Lee Rosen, Ph.D. ("he/him")
Interim Associate Dean for Students
Director of Student Well-Being
Assistant Professor, Department of Psychiatry
The Robert Larner, MD, College of Medicine at the University of Vermont
Lee.rosen@med.uvm.edu
Drop-in sign-up here