April 29, 2020

Duke's IT security offices are issuing a warning to the Duke community after a sharp increase in email impersonation attacks targeting staff and faculty.

In the past week, attackers have impersonated at least 15 Duke faculty members, sending more than 1,200 phishing emails to Duke users. The impersonated faculty came from a wide range of units and departments, including Law, Nicholas School of the Environment, Computer Science, Surgery, Ophthalmology, Economics, Biology, Chemistry, African and African American Studies, Art, Art History and Visual Studies, and Asian and Middle Eastern Studies.

In these phishing scams, attackers set up an email address outside of Duke (such as Gmail) that appears to be a personal email account for the Duke faculty or staff member they are impersonating. The attacker then sends targeted messages to users who may work in the same department as the impersonated faculty or staff member. The messages often begin with a simple request such as, "Are you available?" If a user responds, the attacker will ask for money to be transferred or for gift cards to be purchased and the activation code provided via email.

In the most recent attacks, several Duke users responded to the phishing scams and purchased
about $1,300 in gift cards.

If you receive such an email and are asked to purchase gift cards or asked to transfer funds via wire, please do not respond, and report the issue either using the Report Phish to Duke button or by contacting security@duke.edu [2] or your IT support.

Source URL: https://security.duke.edu/news-alerts/impersonation-attacks-rise

Links
[1] https://security.duke.edu/news-alerts/impersonation-attacks-rise
[2] mailto:security@duke.edu