A malicious entity sent a mass phishing email campaign targeting members of the University of Utah community on Wednesday, August 17, 2022. The email, which contained the subject “Active Account Validation” and signed “IT Help Desk,” prompted users to open a link to validate their email accounts.

The link led to a Google Docs form with questions intended to harvest credentials, including the recipient's uNID and password, which would allow criminals to try to access 2FA-protected resources using their Duo account. Google has removed the form, but for identification purposes, it contained the following fields (note that random capitalizations are potential clues that it is a phishing attempt):

- Full name
- If you have attended Any University/College Before moving down to this University/College Kindly Click YES OR NO
- If Yes, name of Other University/College You have attended Before
- Office 365 Email Of Former University/College You Once Attended

Never authorize Duo pushes that you do not personally request. If you notice an unfamiliar Duo prompt, select the Deny button to block criminals from accessing your account. A flood of Duo code requests or pushes indicate that the criminal(s) have your username and password, and you should change your password.

Although the university’s Information Security Office (ISO) is removing the malicious email from UMail inboxes, we ask that you alert your users, colleagues, and students about the scam.

If you or one of your users received the phishing email, please delete it.

If you or one of your users provided any personal information to the scammer, please log in to CIS, immediately reset your university password, and call your designated central IT help desk to open a “high” urgency ticket with ISO:

- Main campus, 801-581-4000, option 1
- University of Utah Health, 801-587-6000

Screenshot of the phishing attempt message:

Sent: Wednesday, August 17, 2022 2:27 PM
Subject: Active Account Validation

Dear user,

This is to notify all students that we are validating active accounts. Kindly confirm that your account is still in use by clicking the validation link below.

Validate Email Account

Sincerely,

IT Help Desk

Thank you.