A malicious entity sent a mass phishing email campaign targeting members of the University of Utah community on Tuesday, July 12, 2022. The email was sent from noreply@bookstore.utah.edu with the subject “Secure Inbound ID:#####.” The email notified users that their university password was expiring and prompted them to open a link to keep their current password.

The link leads to a landing page that impersonates the U’s Central Authentication Service (CAS) login page for UMail. If a user logs in, they are then directed to a landing page that impersonates the Duo 2FA portal, which requests the user’s Duo PIN.

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

Thank you.