A recent report on internet security threats placed higher education as the second most targeted sector, moving up from the third spot in 2015.

Why? Universities and colleges possess vast amounts of sensitive personal data, such as Social Security numbers, financial aid records, and intellectual property in academic research and through government and industry partnerships. Information security is the No. 1 concern of higher education IT departments for the second year in a row, according to Educause.

The University of Arizona is no exception. Lo Que Pasa reported earlier this month that a recent phishing scam resulted in some UA employees having their paychecks diverted to accounts controlled by cybercriminals. Spear phishing emails, where the phishing email appears to be sent from a known individual or entity to gain your trust, are often sent using a previously stolen identity. These increasingly sophisticated scams have become commonplace, which is why securing information assets has taken on greater importance.

Gil Salazar, the UA's deputy chief information security officer, says that over 130 spear phishing emails have been reported at the University since Nov. 1.

"Cybercriminals are deliberately targeting our institution, trying to get your information and identity," Salazar said.

The NetID password management system, used when you log in to campus online services, is being upgraded to incorporate the latest security best practices and features. Once it is in place, members of the campus community will be asked to change their NetID password (normally done once a year) in order to log in to campus services from the new system.

Derek Masseth, interim chief information security officer, points to some of the tools that University Information Technology Services and UA Information Security have developed and continue to optimize in order to protect the campus community from the consequences of compromised passwords.

- NetID+, the UA's secure method of two-factor authentication, will be required for additional services and systems this year, such as Microsoft Office 365 and the new faculty and staff email and calendar service, UAconnect365, being implemented this spring through summer. NetID+ is already used by a third of the campus community to access the campus virtual private network, the Confluence collaboration service, and some UAccess systems.
- Global NetID+ enforces two-factor authentication for all sites that use UA WebAuth for login, such as CatMail, D2L and UAccess. This is especially critical for protecting UAccess Employee data, since a criminal would be unable to access personal information even if a NetID password was compromised. UA Information Security
strongly recommends enabling Global NetID+ after enrolling in NetID+.

The "plus" in NetID+ refers to a second layer of security—a code sent by text, phone, app or device that authenticates a login beyond the password, protecting accounts in the event of password compromise. Salazar notes, “Banks, email providers and more and more universities are moving to two-factor authentication.”

Masseth recommends that all employees enroll [5] in NetID+ and enable Global NetID+ [6] now to protect their identities and UA accounts. Instructions for setting them up can be found at security.arizona.edu/netid-plus [7].

"This is the new reality of higher education IT," Masseth said. "These changes will put the University and each of us as individuals in a much better security position."

As these security changes are rolled out, UITS will share updates via UAnnounce, the SecureCat Courier [8] newsletter and other official sources.

Visit UA Information Security [9]’s website for more security tips and resources, including phishing alerts and how to spot phishing attempts.

Source URL: https://uaatwork.arizona.edu/lqp/protect-your-identity-netid

Links:
[5] https://webauth.arizona.edu/netid-plus/
[8] http://security.arizona.edu/securecat-courier
[9] http://security.arizona.edu/