UA Launches NetID+ to Provide Stronger Protection for Campus Data

University Information Technology Services
March 2014

Security breaches at higher education institutions pose a real threat to sensitive information on university campuses. To provide additional protection for sensitive data and online services on campus, **University Information Technology Services** [1] is launching NetID+, a two-factor authentication service that will require more than just a single username and password.

NetID+ will require users to verify their identity with "something you know" – like a password – and "something you have" – like a physical device – in order to access your account. According to UITS, the second level of security provided by the two-step login process will help prevent theft and misuse of University data and systems.

NetID+ will be launched April 7 as an optional service for UA employees and students, although UITS will be investigating its mandatory use for various University applications with heightened security requirements.

To opt in to NetID+, users will need to enroll at the NetID+ self-service website at **webauth.arizona.edu/netid-plus** [2]. After logging in with their password, users can then register one or more devices – smartphone, cellphone, tablet or landline telephone – that they wish to set up as a "second factor" authentication.

Once the opt-in process is completed, users can enable the "Global NetID+" setting, which will enforce second-factor authentication for all sites utilizing UA WebAuth or Shibboleth authentication services for login – such as CatMail, D2L and UAccess.

Each time a user who has opted to useNetID+ logs in to aWebAuth or Shibboleth-enabled site with their NetID they will be presented with a "NetID+ Required" message. The message will present the user with a list of all their registered devices, and the methods supported for second-factor authentication – ranging from the **Duo Push** [3] feature of the **Duo Mobile** [4] app, to one-time passcodes delivered via SMS text message or automated voice callback.

To summarize the process, after entering their NetID and password, users will:

- choose device where an authentication code should be sent, like a smartphone or tablet
- retrieve the code sent to their device via push notification, SMS text message or automated phone call
- enter the code into the computer to complete the log-in

"NetID+ will increase the level of security for the campus community and help protect them against the harmful impacts of fraud or hacking attempts," said **Gil Salazar**, senior information security analyst for the University Information Security Office. "For example, in the case of a successful phishing attack, the hacker will not be able to access the account without passing through that second authentication request."

Gary Windham, senior enterprise systems architect for UITS, said NetID+ could provide a dramatic improvement in the UA's cyber security infrastructure. He cited a **Verizon 2013 Data Breach Investigations Report** [5] that states 76 percent of digital security breaches involve weak or stolen passwords.

"Stolen passwords continue to be an attacker's favorite way to circumvent digital security," Windham said. "Ensuring that the user also needs to have something in their possession in order to log in thwarts attackers."

For more information about NetID+ information and instructions for opting in to the service, visit **webauth.arizona.edu/netid-plus** [2].

Links
[1] http://uits.arizona.edu/ [2] https://webauth.arizona.edu/netid-plus [3] https://www.duosecurity.com/duo-push [4] https://www.duosecurity.com/product [5] http://www.verizonenterprise.com/DBIR/2013/