2-1-2019

DUO and Internet Security Policies

Wayne Johnson
Georgia Southern University

Senate Executive Committee Request for Information

DUO and Internet Security Policies

Submitted by: Wayne Johnson

2/1/2019

Question(s):

---

1 Will the requirement to change passwords every 90 days be removed once 2FA is fully implemented? If not, what is the likelihood of a faculty account being hacked with only 2FA in use?

2 What if a faculty member forgets her/his phone or the battery runs out and cannot login to mygsu to access Folio for a class lecture?

3 What if a faculty member does not have a cell phone, does not have immediate access to a landline, nor 2FA backup codes at the time they are logging in? For example, a faculty member could be using a new computer at an out of town conference or in a new classroom.

4 Will 2FA be required for all root/SU users and all members of the President's Cabinet?

5 Will 2FA be required for students also? If so, how will this impact faculty who have a “no cell phone use in classroom” policy?

6 Is this new 2FA requirement intended to truly protect individual faculty accounts or more so to limit access in the event an ITS server with all user's password information is hacked?

7 What is ITS's policy for balancing usability vs. security?

8 Is ITS aware that given the 90 day expiration and non-repeating password requirements, that many users end up writing down their password(s) on a piece of paper? Does ITS consider this end result to be a more secure overall system?

9 What published best practices policies does ITS follow regarding the current password expiration policy and the pending DUO 2FA mandate?

10 Will the backup 2FA codes ever expire?

11 Is a password expiration policy more effective than a strong password requirement policy in controlling unauthorized email, etc access?

12 What happens when there is no access to cell phone signals within a classroom as is the case in most classrooms in the Statesboro IT building?

13 What if a faculty member owns a Windows phone? Is there an app that works for Windows phones?

14 What are the advantages of using DUO over already established 2FA solutions that allow the choice of Google Authenticator/Authy, email, or text codes?

15 Does ITS have a policy regarding use of student USB drives in the office computers of faculty? Could this be a greater security risk than hacking of a faculty email account?

16 Is MyTech Support staffed 24-7/365? What if I am locked out of my account after hours or during university holidays?

17 Are there any plans to improve the DUO interface and usability of the 2FA code enter page?

18 It is obvious that if a hacker gained unauthorized access to a staff account working in financial aid, the registrar's office, human resources, or the bursar's office they would have access to very personal and privileged information. What types of personal or privileged information do non-administrative faculty have access to besides information stored in DegreeWorks?

19 In the year(s) prior to the implementation of the 90 day password expiration policy, how many times was a faculty email hacked via password brute force or some other password cracking tool/technique?

20 In the year(s) since implementation of the 90 day password expiration policy, how many times was a faculty email hacked via password brute force or some other password cracking tool/technique?

21 Considering GS's commitment to shared governance, how did ITS work with faculty senate leadership to develop and vet this new DUO requirement?

Rationale:

It is without question that ITS at Georgia Southern (GS) has worked tirelessly to protect GS students, staff and faculty end users from Internet related security breaches. Their work is such that it is easy to take it for granted until something “breaks”. ITS has be proactive in implementing security policies that attempt to minimize unauthorized access to MyGSU, which most recently has consisted of a 90 day password expiration policy with a non-repeating password requirement. ITS is now planning in March 2019 to require all GS employees to use Two Factor Authentication (2FA), referred to as DUO, in addition to the 90 day password expiration policy. The DUO website (https://its.georgiasouthern.edu/duo/) does address some questions regarding this new ITS DUO requirement, but there are many unanswered questions and concerns from the faculty perspective that should be addressed before full implementation of DUO as well as other data security concerns. We can all agree on the importance of maintaining a secure Internet infrastructure, but it is also important that we strike the best balance possible with our key objective of providing transformative learning opportunities as we advance knowledge at the new Georgia Southern.

Response:

2/22/2019: The SEC did not approve this to move to the floor. If you would like to revise the RFI to a length that would be answerable during a Senate meeting, please see below.
Based on the rationale included regarding ITS's role in Shared Governance, the appropriate question to pose in the RFI would be:

"7. What is ITS's policy for balancing usability vs. security?"

Questions with the level of technical detail demonstrated in the remaining 20 questions should be first directed to appropriate departments. ITS posted the following in May 2018:

"Have questions about two-factor authentication or need technology support? Our MyTech Support representatives can help. Call (912) 478-2287 or use one of our other contact methods [https://its.georgiasouthern.edu/about/contact/]."

If the department was unwilling to answer these questions, you should then request information through the Senate.