Two Factor Authentication

The Texas A&M University System’s Enterprise Software Initiatives office has implemented two factor authentication as part of the Single Sign-On (SSO) logon process to better protect personal, sensitive and confidential information.

Two factor authentication is a security technique that supplements your SSO password – something you know – with a second, tangible identification factor or device – something you have – such as your office or cell phone.

Effective July 21, 2015, two factor authentication will be required for employees with administrator roles or who have authority to access or edit potentially sensitive data in SSO applications, including applications that touch on HR or payroll-related information.

Most HR Liaisons will be required to use two factor authentication and can opt-in sooner to get familiar with the system. You can choose to opt-in from the employee Profile tab in SSO.

Employees in your department may also be required to use two factor authentication, or they could choose to opt-in as an additional security measure.

FAQs on SSO security and two factor authentication is available here http://it.tamus.edu/sso/frequently-asked-questions/

SSO Applications with Two Factor Authentication

The below-listed SSO applications – and all users with roles in those applications – are subject to two-factor authentication, except for the roles as noted:

- BBP Utilities; HRConnect; UIN Manager; UIN Search; Single Sign-On Administration
- DW Report Portal; Endowment Reports; File Depot; HUB Quarterly Reporting; SECC Admin
- Monthly Payroll (except for Department Approver)
- TimeTraq, LeaveTraq, TrainTraq; iBenefits, Time & Effort (except for Employee, Manager & Department Approver)
- Event Registration (except for Department Administrator)

Helping Employees with Their SSO Logon

HR Liaisons who are an SSO Department Administrator can:

- Reset a user’s password, and now also,
- Delete a user’s device enrolled in two factor authentication in the event it is lost or no longer valid

Please always verify a user’s identity before resetting their online security functions or password.

FAQs on SSO security and two factor authentication is available at http://it.tamus.edu/sso/frequently-asked-questions/