From: Office of the President
Sent: Monday, July 06, 2015 9:48 AM
To: Faculty List; Staff List
Subject: Message from President Turner

Recently added self-service capabilities to my.SMU have created new conveniences for University employees, as well as new opportunities for online theft and fraud. In May and June 2015, several employee accounts were compromised via a phishing message that allowed a cybercriminal to modify the employees' direct-deposit information.

In light of the increasing number of information security incidents on college campuses, SMU is taking the proactive step of requiring data security and privacy awareness training for all employees. The training should take less than 30 minutes and will become an annual requirement.

You will receive additional information about the training in the following days. Please watch your SMU e-mail for a notification from Law Room that the tutorial has been assigned. Please complete the training as quickly as possible, but **no later than 60 days after assignment**.

SMU plans to deploy two-factor authentication for all users of my.SMU. Two-factor authentication adds protection beyond username and password authentication; familiar examples include the combination of a bank card and correct PIN number needed to complete an ATM transaction, or an e-mail verification code required to change a website password.

SMU's Office of Information Technology (OIT) has been sending simulated phishing messages to all employees over the past two years to provide directed training to mitigate the threat of phishing messages. In the past two years, SMU OIT has reduced the success rate of these messages from 40 percent to 11 percent. In addition, the University stopped more than 350 million SPAM messages and more than 50 million cyberattacks, not including SPAM and phishing, in the past 12 months.

A number of national incidents illustrate the importance of ensuring that all University community members are well versed in protecting their information. In February 2014, the University of Maryland announced it had lost the personal information of more than 300,000 current and former students, staff and faculty members. In March 2015, Auburn University announced a cybersecurity breach that affected 300,000 individuals, including prospective students. Information lost included Social Security numbers and other information.

The direct costs for remediating such a breach at SMU could start at about $50 per individual record lost, whether those contain student or employee information (credit card, SSN, etc.). This does not include the impact to the University for losses of reputation, prospective students, or alumni donations.

Please contact SMU's OIT Help Desk at 214-768-4357 (214-SMU-HELP) with any questions about this program or its content, or SMU Human Resources at DevelopU@smu.edu regarding course assignments and access to training. Thanks for your support.