

POSSIBILITIES

SPRING 2019

Division of Information Technology

ABOUT THIS ISSUE
.....

The Division of IT is excited to bring you our 2018 Annual Report, "Transforming Today and Tomorrow," highlighting our dedication to transformational learning, innovation and impact on the world.

The report can be found online at u.tamu.edu/annualreport.

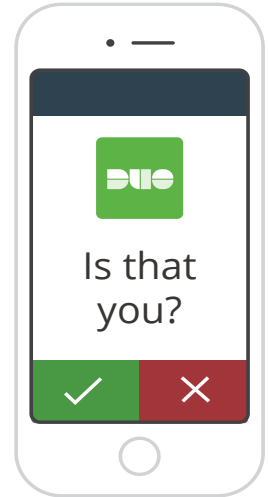
Be sure to follow the Division of IT throughout the year on Twitter [@TAMU_IT](https://twitter.com/TAMU_IT) and Facebook at facebook.com/tamuIT.

JUST DUO IT

Don't Forget: Register for Duo by April 15

April 15 isn't just tax day this year, it's also Duo Day – the deadline for Texas A&M faculty and staff to register for Duo NetID Two-Factor Authentication.

Two-factor authentication adds an additional layer of security to ensure you are the only person who can access your accounts by requiring a confirmation on your mobile device (or answering a phone call) in addition to your password. If you haven't registered yet, do so now at duo.tamu.edu.



Mark your calendars

April 15 is the deadline for all employees to register for Duo!

Enroll in NetID Two-Factor Authentication at duo.tamu.edu

TWO 
IS BETTER THAN **ONE...**

The Division of IT: "Transforming Today and Tomorrow"

How is the Division of IT transforming today and tomorrow? Find out in the 2018 Annual Report, available online at u.tamu.edu/annualreport.



892K VIRUSES

blocked by the campus
firewall every month

10.1 MILLION

emails inspected daily for
spam, phishing & viruses



OVER 4 MILLION

Wi-Fi Sessions Secured each day



OVER 53TB OF DATA

*transferred over the network
each day during the semester*

THE DIVISION OF IT PROTECTS



227,000
accounts



20,000
exchange mailboxes



106,000
devices

in an average moment in time

Introducing the
AGGIE TECH HELP SKILL
for Alexa



Division of IT wins

"BEST OF TEXAS" CYBERSECURITY AWARD



Capstone project students and Division of IT members helped bring an Alexa skill proof-of-concept to life. Pictured from left to right are students Jack Swink, Aaron Blasband and Justin Bevelo; Lacey Baze, Associate Director of Product Strategy and Communications for the Division of IT; student Joey Sapp; and Bobby Bernshausen, Communications Coordinator for the Division of IT.

REAL-WORLD EXPERIENCE

Capstone Project Brings Familiar Voice to Campus

Note: This article is from the 2018 Annual Report, "Transforming Today and Tomorrow."

"Alexa, how do I change my NetID password?"

That's just one of the questions users can ask Amazon Alexa using the new "Aggie Tech Help" skill developed by the Division of IT. Four students from the Department of Computer Science and Engineering created the proof-of-concept as part of their senior Capstone project.

Justin Bevelo, Aaron Blasband, Joey Sapp and Jack Swink were the "Texas A&M Alexa Development Team" in visiting professor Mahima Agumbe Suresh's course in the Spring 2018 semester. Dee Childs, Vice President for Information Technology and CIO, asked the students to design a skill that would serve as an extension to Help Desk Central by answering tech questions.

Bevelo, who now works as a consultant at the management firm Credera, said the experience helped when he entered the "real world."

"This project was my first client-based assignment where I was expected to communicate effectively with the client," he explained. "This experience definitely helped prepare me for my current role with Credera."

Suresh, who is now an assistant professor at San Jose State University, said the team learned much more than coding during the project.

"From a project management perspective, the students learned how to gather requirements, divide responsibilities and work as a team," she said. "The technical skills the team learned included Alexa skills and web development."

USE TECH SAFELY

Don't Let Gadgets Compromise Your Security

Would you leave the back door of your home or apartment open while you're gone? Then why leave yourself vulnerable to online intruders?

As we continue to add devices to the internet – from light bulbs and refrigerators to doorbells and thermostats – it's a good idea to make sure your devices are secure.

Here are some things you should do before connecting any device:

- **Immediately change the default password.**

Be sure you set a strong password of eight or more characters, including upper and lowercase letters, numbers and special characters.

- **Install any available updates.**

The device may have sat in a warehouse for a while and the default software may be out of date or contain vulnerabilities.

- **Ensure automatic updates are enabled.**

This will keep your device up-to-date with security updates and new features.



- **Disable location services when not needed.**

- **Turn on PINs and unlock patterns.**

If your device has these extra levels of protection, be sure to enable them.

- **Turn off network/internet access for devices that don't need it.**

Check your device, as these settings are often turned on by default.

