# POSSIBIL**IT**IES

## ABOUT THIS ISSUE

Thanks to you, Texas A&M University successfully navigated a year of adversity and uncertainty.

In this issue of PossibilITies, we'd like to take a look back at how the campus community faced the

challenge head on and emerged strong, determined and prepared for the future.

### KEEP YOUR HEAD IN THE CLOUD

## Microsoft 365 Increases Productivity at Home and Office

Hybrid work and learning were – and continue to be - crucial to success. Thanks to Texas A&M's integration with Microsoft 365, new tools make those efforts more efficient and productive.

**Microsoft Teams**, the collaboration tool available to all campus members, now offers **real-time transcriptions** for scheduled meetings. Transcriptions can be saved with recordings for captioning. In April, Microsoft will release **Dynamic View** for Teams to arrange content and participants for better viewing experiences. A new presenter mode will allow hosts to customize how things will look for participants. Hosts will also have the ability to download attendance reports at the end of a session.

The new **Microsoft Editor** serves as a virtual writing assistant by offering advanced grammar and style refinements like clarity, conciseness, formality, punctuation, vocabulary suggestions, synonyms and more. **Editor** works directly in Word and Outlook and has browser extensions for **Microsoft Edge** and **Chrome**.

### More to come ...

To take advantage of Microsoft 365's capabilities, Texas A&M Exchange email will begin moving to Microsoft 365 in the cloud this summer. Once complete, employees will have access to:

- **Microsoft To-Do** — This planner makes creating, sharing and organizing tasks easier on your desktop, laptop and mobile devices and connects to Outlook.

- **Bookings** — Makes scheduling virtual and in-person meetings more streamlined.

- **FindTime** —  Allows you to find the perfect meeting time based on the availability of all attendees.

Microsoft 365 training will be available to the campus community this summer. Stay tuned for details.

# Annual Report Chronicles Ways University Was Prepared, Focused, Resilient.

Protecting the health, safety, data and technology of campus was crucial during the pandemic. Everyone contributed to ensure day-to-day operations of the university — and life in general — continued. Those efforts are highlighted in the **2020 Division of Information Technology's Annual Report**: Prepared. Focused. Resilient.

## Prepared.

- Network attacks against the university plummeted at the onset of the pandemic then increased to almost 10 times pre-lockdown levels. The heightened threat level remained manageable thanks to the **Cyber Security Integration (CSI) tool** developed by the division.

- The division helped researchers face the challenges of 2020 with two platforms designed to harness the full potential of cloud-based resources: the **Secure Technologies for Aggie Researchers (STAR)** and **Aggie Innovation Platform (AIP)**.

## Focused.

- In partnership with TAMU Health, the division developed a **COVID-19 dashboard** for the campus community to help university leaders track COVID cases and make crucial decisions regarding campus safety. The tool collects data from multiple sources, including **self reporting** and **testing data** from campus walkup locations. The dashboard has been visited over 350,000 times since its launch.

- In June, the Division of IT created a contact tracing center in partnership with the School of Public Health (SPH). Three large rooms of Clinical Building 1 were converted for use by approximately 50 staff members to call anyone who **self reported** a positive test result or symptoms and those with whom they made contact. The tracing center became vital when the Provost asked the SPH to begin random testing of the Texas A&M community.

- When the university announced the return of in-person classes for the fall, the Division of IT worked with university leaders to ensure social distancing by **outfitting many non-traditional spaces for learning**. This required the installation of Wi-Fi in meeting rooms, theaters, arenas and parking lots across campus.

## Resilient.

- The new **Code Maroon Mobile App** was released, allowing anyone to receive Code Maroon emergency alerts. The app features a **Mobile Blue Light and a Friend Walk feature** that can be used anywhere.

- Texas A&M's **Accessibility Conformance Evaluator (ACE)** proved invaluable during the pandemic by making it easier for campus members to find and evaluate accessible Electronic Information Resources.

# The Division of IT: "Better Together"

## Protecting Texas A&M

*On average, the Division of IT protects:*

**171,768**
Mailboxes

**237,000**
Accounts

**705,379**
Active Identities

## Staying Connected

*Texas A&M University is among the top 10 largest campuses in the nation and needs one of the largest networks to support it.*

**7,767**
Wireless access points on the College Station campus

**78,000**
Devices on the Texas A&M network each day

**19.3 million**
Square feet of wireless coverage on the College Station campus

**115.26 TB+**
Data transferred over the network each day during a semester

## Securing Our Information

*The Division of IT secures and protects data essential for the teaching and research functions of Texas A&M.*

**28 million**
Viruses blocked each month by the firewall

**23.5 billion**
Cyber and malware attacks blocked each month

**1 million**
Wi-Fi sessions secured daily

**240 million**
Emails inspected daily for spam, phishing and viruses

# Protecting the University at the Office and from Home

Unfortunately, it was "business as usual" for most cybercriminals during the pandemic. While institutions of higher learning are always major targets, a recent FBI "news flash" warned of an increase in ransomware attacks.

Michael Denison, Texas A&M Assistant Director of Cyber Defense, said most ransomware attacks originate in phishing emails. While over 23.5 billion cyber and malware attacks are blocked each month at Texas A&M, he said users need to be vigilant when checking messages.

> " First and foremost, if you receive a message from someone you don't know, be extremely careful if you must open it," he said. "The message may contain an offer, a promise of a prize or just ask you to click and view an invoice or package tracking information. If you aren't expecting anything of this nature, especially if it has an attachment, the safest thing is to just trash it. "
>
> **– MICHAEL DENISON, TEXAS A&M ASSISTANT DIRECTOR OF CYBER DEFENSE**

## Stay up to date

When using a home computer, be sure to keep all software (especially anti-virus programs), operating systems and drivers up to date. Firewalls should also be used for extra protection. Dennison explained that while IT groups take care of this at the university, everyone needs to make sure their home computers are protected as well.

"You'd be surprised at how many home users are using operating systems that are no longer supported, like Windows XP," Dennison pointed out. "Since Microsoft no longer maintains this operating system, they are prone to attacks. Of course, Macs and Linux computers are prone to attacks as well, so they also need to be up-to-date."

## Two is better than one

Duo NetID Two-Factor Authentication plays an important role in protecting the university. To take advantage of this extra security, you can also use the mobile Duo App for two-factor authentication with personal accounts such as Facebook, Instagram, Snapchat and others.

## Play the game

To keep cybersecurity awareness at the forefront, the Division of IT hosts a free online game and campaign every October and plans are underway for the 2021 event. If you'd like to brush up on your cybersecurity knowledge, past games can be played at u.tamu.edu/games.