IT Overview

May 2020

Dale Vickers, Chief Technology Officer

COVID-19 Projects

- Really proud of the way IT staff rose to the challenge – huge progress in all areas – sometimes making stuff up as we went trying to support Faculty, Staff, Students and Administration – in some cases doing what we'd been told can't be done

- Some of these things made it into the Admin Services Quarterly report – additional items on IT Blog at https://www.mtsac.edu/it/blog.

- The online form to request equipment and VPNs is now off and all requests for equipment, VPNs, and technical assistance are going to Help Desk. Through the web form, IT processed 641 requests for equipment and VPN accounts for employees.
    - Additional equipment needs should go to the Help Desk.
    - Any urgent needs, please contact me and/or Ron.

- Network outage planned for Friday, May 15, from 5:00 a.m. until at least 7:00 a.m., to repair a firewall issue related to the pandemic caused by network traffic changes and performance issues due to VPN and work from home access.

Preparations for Summer and Fall

- Considering factors that may assist with opening certain labs and services such as
    - Distancing of computers
    - Cleaning protocols
    - Staffing needs

- Supply Chain Issues – Even orders placed in Jan/Feb took forever.
    - Computer/Laptop Orders
        - Vendors are reporting shortages and long lead times for delivery.
        - Laptops are in-demand by schools, businesses, and home users.
    - Related Pheripials
        - WebCams
        - Printers – Question on College Supplying these for home use?

Academic Technology and Technical Support
Security and Infrastructure
May 2020

Ron Bean, Director Academic Technology
Chris Schroeder, Director Infrastructure & Data Security
Lee Jones, Manager Technical Support

Academic Technology and Technical Support

- Collaborating with Student Services on preparing for the summer distribution of student laptops. Anticipating delivery of 1,000 laptops and scheduling technicians to complete the setup.
- Supporting academic departments with virtualized configurations to allow students to access processor-intensive software like CAD and fashion design.
- Provided access to Cranium Café to additional counselors and other departments.
- Prepared and distributed over 500 computers to staff and students.
- Since March 23, IT Help Desk has processed 1,825 requests for assistance. With the start of registration, we are primarily receiving requests from students.
- IT Help Desk and FCLT have collaborated on including FCLT request tickets in the same system. A new button/form for faculty to request cross-listing Canvas courses is available. FCLT is also adding Knowledge Articles to https://helpdesk.mtsac.edu
- Telework and equipment requests are now using a button/form on the IT Help Desk portal instead of the SmartSheet web form.
- The Emergency Operation Center was prepared in March. Four laptops and six phones are in a state of readiness for use (last checked on Thursday, May 7th)

Security and Infrastructure

- The team is issuing VPN accounts, as needed. The current daily connection count is above 700. To accommodate this explosive growth, an unlimited license was purchased, and network architecture was re-worked to provide secure IP addresses to accommodate all the connections.
- Telecom Team continues to provide phone solutions for off-campus employees. The MiCollab solution allows the employee's cell phone caller ID to show 'MTSAC.' Additional licenses may be needed for this feature due to increased work from home requests.
- IT is testing two-factor authentication (2FA) with O365. Please see attached Appendix A regarding passwords and 2FA. This added security measure is needed due to increased credential theft from phishing attacks related to the pandemic.
- IT is testing and rolling out Azure Active Directory management of computers via hybrid joined devices. This method will enable management of off-campus devices to be remotely managed and tracked.

- System software upgrades are being performed on the phone system. These prerequisite upgrades are required before initiating the migration of the phone system from Primary Rate Interface (PRI) to Session Initiated Protocol (SIP) with Spectrum. The completed project will reduce operating costs and provide phone system redundancy to better serve the College with regular and emergency operations.

Enterprise Application Systems
IT Project Management
May 2020

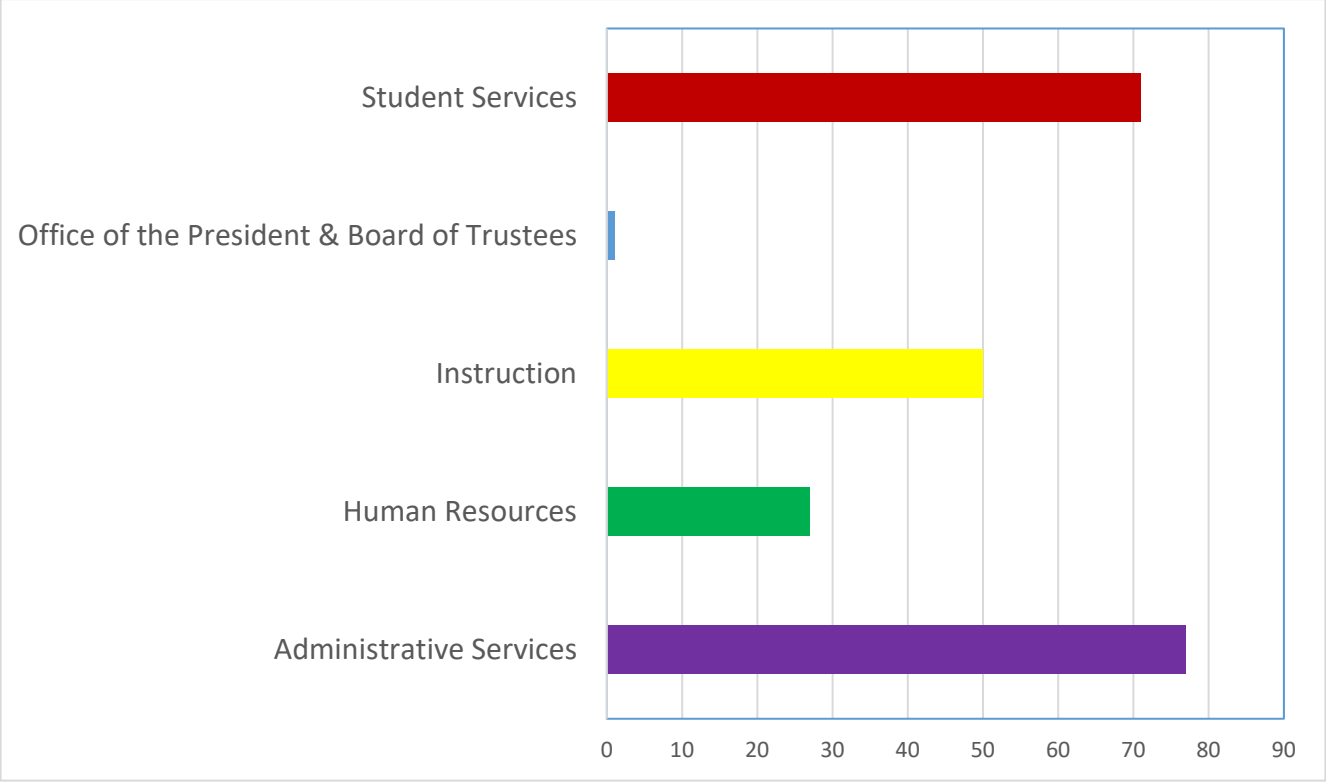
Antonio Bangloy, Director Enterprise Application Systems
Monica Cantu-Chan, Director IT Projects
Chuong Tran, Asst. Director Application Support and Development
Eric Turner, Asst. Director Web and Portal Services

- In response to COVID-19, numerous programming projects were completed or are in process including:
    - Option for pass/no pass
    - Enabling students to register up to the original max units allowed after dropping classes with Excused Withdrawal.
    - Temporarily extend SPOT certification for faculty so classes can be taught online.
    - Completed programming to allow students to excuse withdraw and receive refunds without it counting negatively on their transcript.
    - Completed the noncredit online application to enable noncredit students to apply online.
    - Completed programming to automate the conversion of "W" grade to "EW" with an accurate calculation of refunds.
    - Completed programming to excuse withdraw (EW) students that belong to "Cancelled" classes – (classes that were not transitioned to online teaching).
    - Completed programming to allow dual enrollments in Winter 2020 to drop with EWs and changing grading option online. Typically, dual enrollment students in the Winter term have to submit a petition to drop after the regular term ends in February.
- In partnership with Student Life and Cashier's Office, completed the opt in/out online process for $2 Student Representation Fee. This is in compliance with AB 1504.
- In partnership with the College-wide electronic forms committee, we are in the process of researching and implementing an electronic signature process. The committee is asking for campus assistance by completing the Online Form Submission.
- IT, in partnership with Fiscal Services, started the implementation process for Chrome River, the College's new travel and expense reporting module. Projected implementation is by the end of 2020.
- Business Analysts are helping various departments transition paper forms that don't require official signatures to online forms with workflows. Please contact Monica Cantu-Chan if any assistance is needed.
- A new area was unveiled in the Portal for Student Services to advertise their services. This new area appears at the top of the Portal homepage, is brightly colored, and is the first thing students see upon entry.
- In collaboration with FCLT, new functionality was added to Canvas, including:
    - A Student Hub that features important links to resources students need as they transition online.
    - Labster that helps faculty teach science laboratory lessons online.

    - Screencast-o-Matic that allows faculty to take screenshots of their lessons and post them in Canvas.
    - Blackboard Ally that automatically checks for common accessibility issues and provides alternative formats for all learners, including braille and audio options.
- A cross campus team is reviewing options for live captioning of online sessions to meet accessibility requirements. The current recommendation is live captioning with Verbit and auto captioning with ConexEd, the same vendor as Cranium Café that is used by our Counselling Department.
- See attached Appendix B for security related to issuing student email accounts.

Completed Requests

January 2020 through April 2020



Passwords Are Like Toothbrushes

Change yours often - 81% of breaches involve stolen or weak passwords [5]. Keep your password fresh and change it regularly.

Don't share it – 25% of all breaches for the Educational sector involved account compromises from web application attacks. These attacks were mainly phishing links leading to fake login pages [5]. 38% of users admitted to sharing password with colleagues, which add to the problem of compromised accounts [2].

Choose a good one – A password should be complex and greater than 8 characters [3]. A good password should be a memorable phrase, like 'The sky is full of stars!'. A difficult or bad password is hard to use.

Don't reuse an old one – Passwords should not be reused for 4 cycles but is best if they are never reused again [1].

Don't share it – Sharing a Netflix or Hulu login is far different from sharing a work account containing sensitive information like social security numbers. One is entertaining, while the other puts the College at risk of state and federal privacy laws and data breaches. As with your toothbrush, don't share your accounts and passwords.

A Password Sharing Case Involving Data Theft

David Nosal was a former employee of Korn and Ferry. After leaving the executive search firm to start his own competing business, he was able to convince his friends and former colleagues to send confidential information, including sharing credentials. Nosal was actively soliciting help from former colleagues to access protected systems from his former employer, despite signing non-disclosure and non-compete agreements. The proprietary data lost by Korn and Ferry included source lists, names, and contact information. Nosal was charged on 20 counts, including trade secret theft and mail fraud [4].

Embracing Two-Factor Authentication

Two-factor authentication can prevent use of leaked or shared credentials. When enabled, logins require the username and password in addition to something in the account owner's possession such as a token to complete authentication.

Employing two-factor authentication would eliminate the risk of compromised or shared accounts being usable to non-account owners. This includes 81% of compromised accounts and 38% of shared accounts [5].

The challenges for College-wide deployment are the support and onboarding of accounts and services. A successful rollout is manageable through batched deployments and training of small cohorts through the onboarding process. Office 365 and Exchange can be leveraged to onboard the college user-base with two-factor authentication. After the initial onboarding and deployment with Office 365 is complete, rollouts of other sensitive services pared with two-factor authentication will be easier to support with an experienced user-base.

References

1. *CCC Information Security Standard.* (2013, September 1). Retrieved from CCC Security Center: https://cccsecuritycenter.org/policy/policy-templates?download=70:ccc-information-security-standard

2. *Infographic: Security Breaches from Compromised User Logins*. (2016). Retrieved from IS Decisions: https://www.isdecisions.com/security-breach-infographic-compromised-login/

3. *NIST Special Publication 800-63B Digital Identity Guidelines*. (202, February 27). Retrieved from National Institute of Standards and Technology: https://pages.nist.gov/800-63-3/sp800-63b.html

4. Stephen M. Byers, M. A. (2016, July 18). *United States v. Nosal: Keep Your Friends Close, but Your Passwords Even Closer*. Retrieved from Trade Secret Trends: https://www.crowelltradesecretstrends.com/2016/07/united-states-v-nosal-keep-your-friends-close-but-your-passwords-even-closer/

5. *Verizon 2019 Data Breach Investigations Report*. (2019). Retrieved from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Security Related to Issuing .edu Email Accounts [1]

We have found several spamming methods that bad actors use when filling out OpenCCC Apply. One thing evident is that they all need to have a consistent way to track their fake personal emails (PE).

Several examples of what we have seen:

1) Incremental method (all emails belong to different names)

   Jmountie111@gmail.com
   Jmountie222@gmail.com
   Jmountie333@gmail.com

2) Rotational method (all emails belong to different names)

   Jmounti.e@gmail.com
   Jmount.ie@gmail.com
   Jmoun.tie@gmail.com
   Jmou.ntie@gmail.com

3) Bulk method (all emails belong to different names)

   Name: Joe Smith Email: Jmountie@gmail.com
   Name: Jean Rogers Email: Jmountie@gmail.com
   Name: Roger Rabbit Email: Jmountie@gmail.com
   Name: Anne Lowe Email: Jmountie@gmail.com

What is the ultimate solution? [2]

We as an institution need to revisit and change our process regarding supplying new students with"student.mtsac.edu" email address. Currently, getting a Mt. SAC student email address is easy. When a prospective student applies via OpenCCCApply, an automatic "Acceptance" is assigned when California Residency is met. And because of the "Acceptance" status, the prospect gets a Mt. SAC email address.

What will make more sense, per IT's stand point, is to assign a Mt. SAC email address only if the prospect decided to either register or made payments. If this gets applied, I

expect a decline on spam applications. However, this will mean that all email communications prior to registration (or first payment) need to be sent to their personal email (PE) accounts.

How about spam applications that are already in our system? This can be taken care of by a "Retention Policy". We should be able to disable student accounts if there are no activities in their accounts for the last two major semesters (Fall and Spring). Re-activation of these accounts can happen once another OpenCCCApply application is received. This process is consistent with our current Registration Eligibility process that Admissions and Records has established a long time ago.

What are we currently doing to mitigate this issue while awaiting implementation of the ultimate solution?

1. We have identified the different bad actors that use the top three methodologies mentioned above, and disabled their student email accounts.
2. We had a meeting with the Tech Center's Support Center, and decided to beef up the SPAM rules that are specific to MtSAC.
3. We are sending the spam files to Support Center, so that they can continue to add the spam applications in to their main spam filter. Other schools will also benefit from the files we are providing the Tech Center.
4. We are in the process of creating programs or engines that will filter spam applications from our staging table after extracting the applications from OpenCCCApply. This will reduce the spam applications significantly (but not eliminate totally) before being uploaded into Banner.
5. We have established a team of three who will be rotating to monitor the spam applications.

References

1. *Mt. SAC President's Cabinet Action Notes.* (2020, February 25). Item 2. https://www.mtsac.edu/president/cabinet-notes/2019-20/CabinetActionNotes022520.pdf
2. *CCC Information Security Center.* (2020, February). Tutorial: Restricting .edu Email Access: https://www.mtsac.edu/president/cabinet-notes/2019-20/04cccapply-whitepaper-tutorials-02042020.pdf