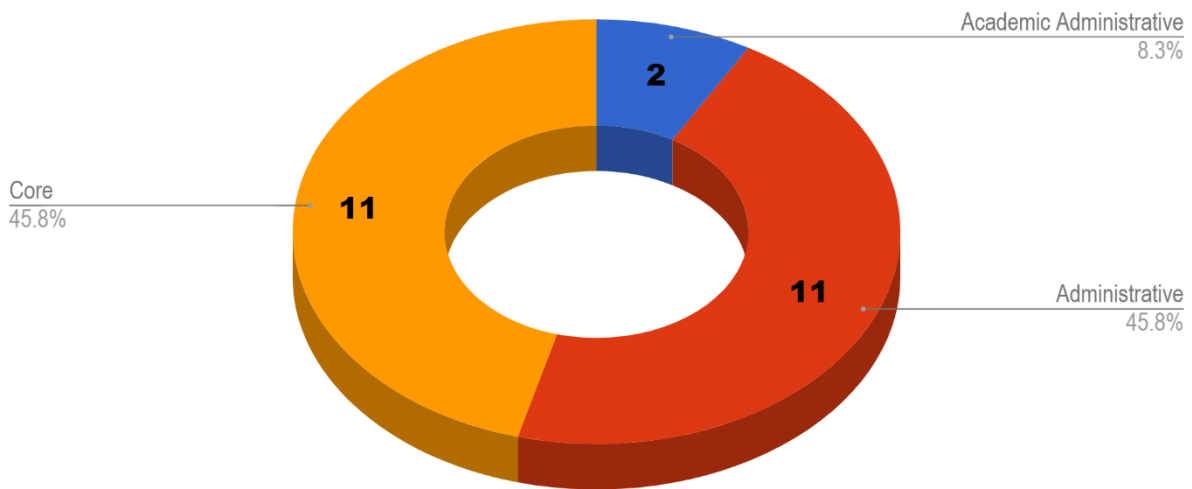


Division of Information Technology Report
Academic IT Committee
March , 2020

Project Portfolio Updates

24 DoIT Projects Currently In Progress

DoIT Projects In Progress by Project Category

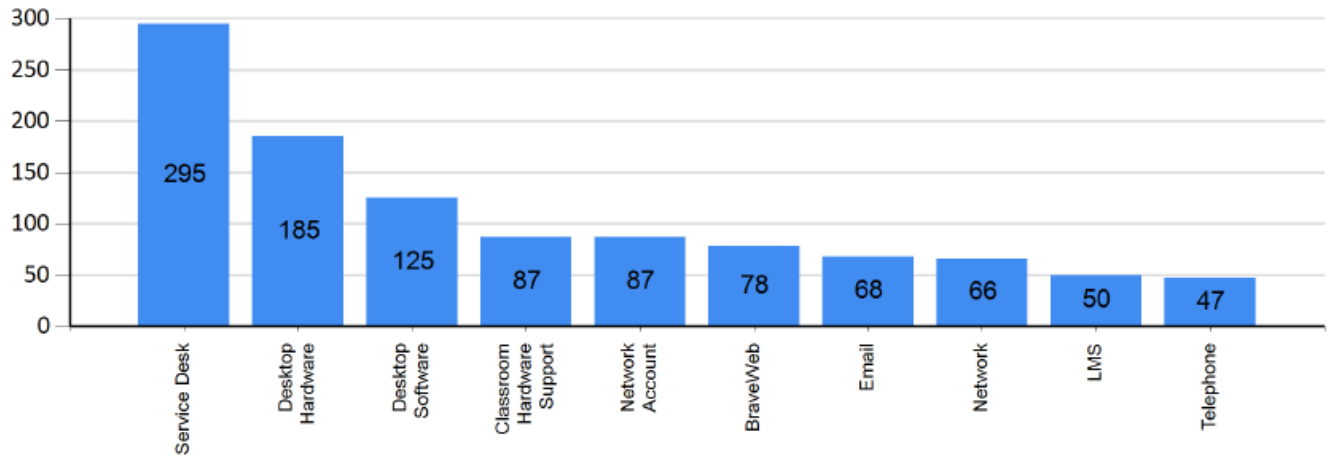


48- Completed Projects FY 19-20

Projects and Efforts of Academic Interest

- **Access to Online Account Center for Prior Students Project** – The Division of Information Technology has partnered with the Controller's Office to create an application that will allow inactive students to make a payment using a credit card through the online account center. The project is scheduled to complete May 2020.
- **User Data Backup Solution Research Project** – The goal of the User Data Backup Solution Research Project, is to work with campus stakeholders to research the various options for user data backup. Once options have been identified, the team will select a tool based on user feedback and implement the best tool to automate backups for user's data. Implementation of a tool will reduce the risk for data loss due to current manual process. The project is scheduled to go live summer 2020.
- **Incident Services – January 2020**

Incident Services - Top 10



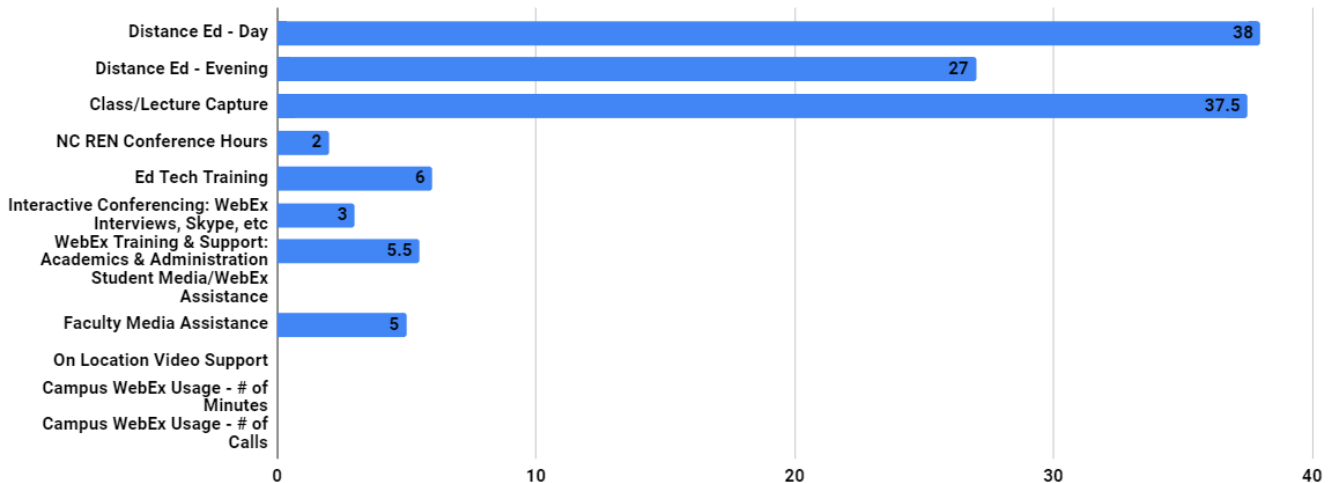
Number of Incidents Resolved in January 2020: 1090

Calls Presented to the Help Desk January 2020: 1456

Interactive Video Facility

The Interactive Video Facility provides services to the campus community in a variety of service categories. Please see the chart below depicting the number of hours of service provided during this reporting period in each category.

January 2020 IVF Hours of Utilization and Support



Canvas Support Tickets to Instructure by Type – January 2020

Email	Live Chat	Online Submission	Phone	Total

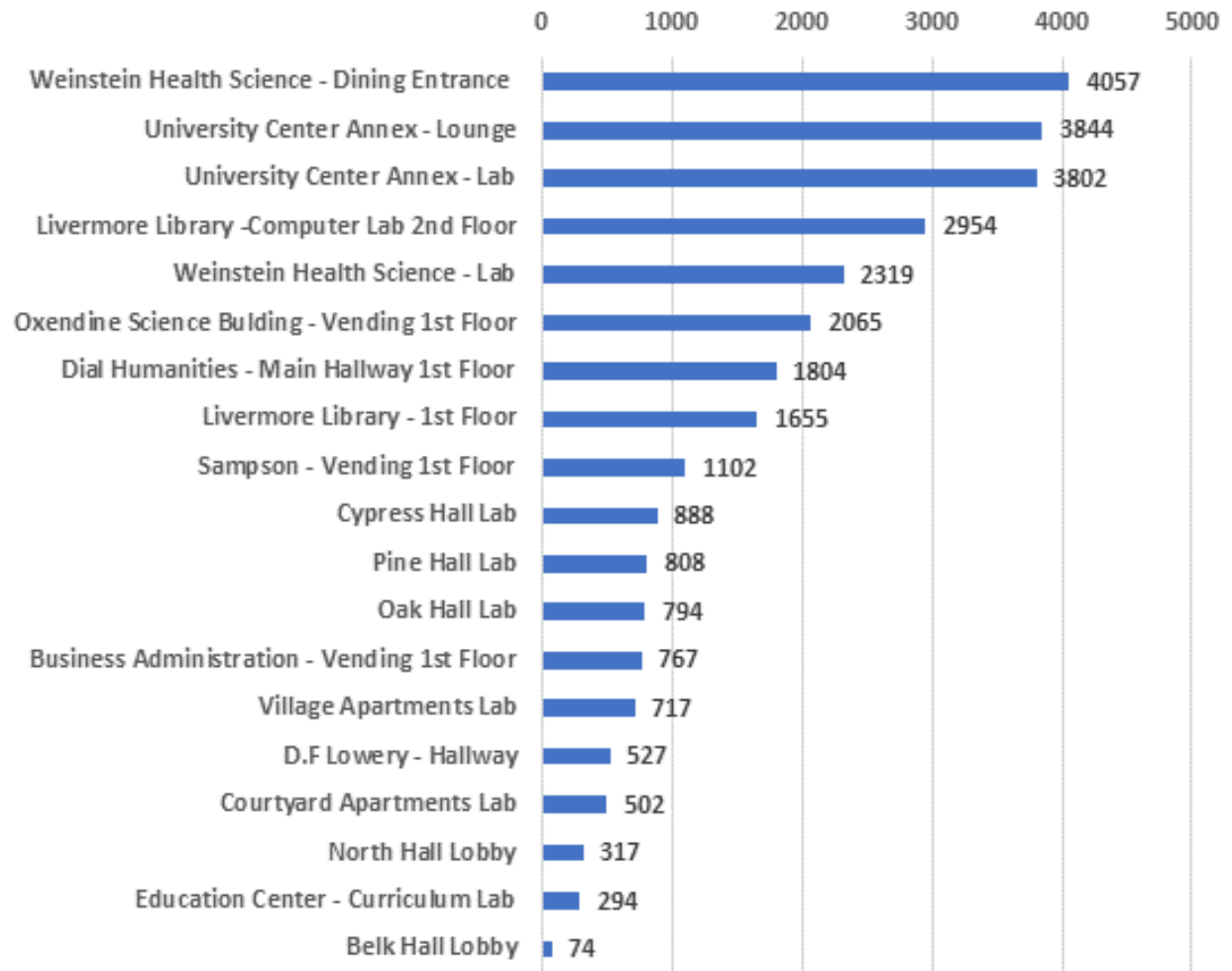
1	36	24	268	329

*DoIT will continue to work with Instructure (the Canvas vendor) to gather appropriate data on their support services and our campus's experience.

WEPA Kiosk Print Station Report – January 2020
















	Total Number of Pages Printed	Mono Pages Printed	Color Pages Printed
Campus Access	25,190	19,883 (78.93%)	5,307 (21.07%)
Residence Hall Access	4,100	4,100 (100.00%)	

WEPA Comparison January 2020



IT Security Summary Report

Executive Email Summary – February 2020

Overview > Incoming Mail Summary ✕		
Message Category	%	Messages
 Stopped by Reputation Filtering	84.6%	15.7M
 Stopped as Invalid Recipients	0.0%	2,852
 Spam Detected	0.8%	152.3k
 Additional Spam Detected by Intelligent Multi-Scan	0.0%	3,958
 Virus Detected	0.0%	3
 Detected by Advanced Malware Protection	0.0%	5
 Messages with Malicious URLs	0.0%	1,424
 Stopped by Content Filter	0.3%	64.0k
 Stopped by DMARC	0.0%	0
 S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:		85.8% 15.9M
 Marketing Messages	4.2%	777.0k
 Social Networking Messages	0.7%	134.7k
 Bulk Messages	3.6%	677.8k
Total Graymails:		8.6% 1.6M
 S/MIME Verification/Decryption Successful	0.0%	0
 Clean Messages	5.6%	1.0M
Total Attempted Messages:		18.6M

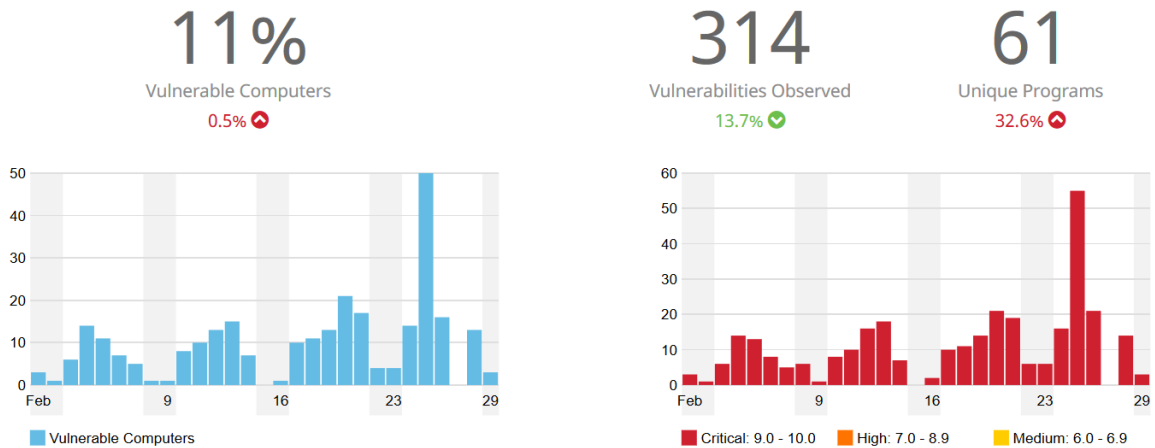
The above graph and tables show the Incoming Email Summary for February 2020. Of the 18.6 million attempted messages in that time frame, only 1 M were considered “clean messages”. While not malicious, “Graymail” accounted for 1.6M messages. These are emails that from social media, bulk email and various marketing emails.

Vulnerabilities – February 2020

The first chart in blue shows the number of computers with vulnerable applications with a CVE (Common Vulnerabilities and Exposures), per day and the number of critical, high, and medium severity vulnerabilities within these applications per day. The second chart in red shows the number of vulnerable applications that have been executed, moved, or copied, and the number of vulnerable university owned computers.

Vulnerabilities

This shows the number of vulnerable applications that have been executed, moved, or copied, and the number of vulnerable computers. If an application with known vulnerabilities is recorded in the [Common Vulnerabilities and Exposures \(CVE\)](#) database, that information is displayed. The charts show the number of computers with vulnerable applications per day and the number of critical, high, and medium severity vulnerabilities within these applications per day.



Threat Root Cause – February 2020

This graph and chart show the software most used to introduce malware into the UNCP network. Firefox, a very popular browser, has assumed the number one position. With cloud resources, including file storage, email, file sharing and other services, it is understandable that browsers would be the key vector for malware.

Threat Root Cause

This shows the applications that have been observed introducing the most malware into your environment within the reporting period. With this information, you can quickly identify applications that are frequently utilized by malware to remain resident on — or gain access to — computers in your environment. The (other) entry is an aggregate of all other applications that have introduced malware into your environment.

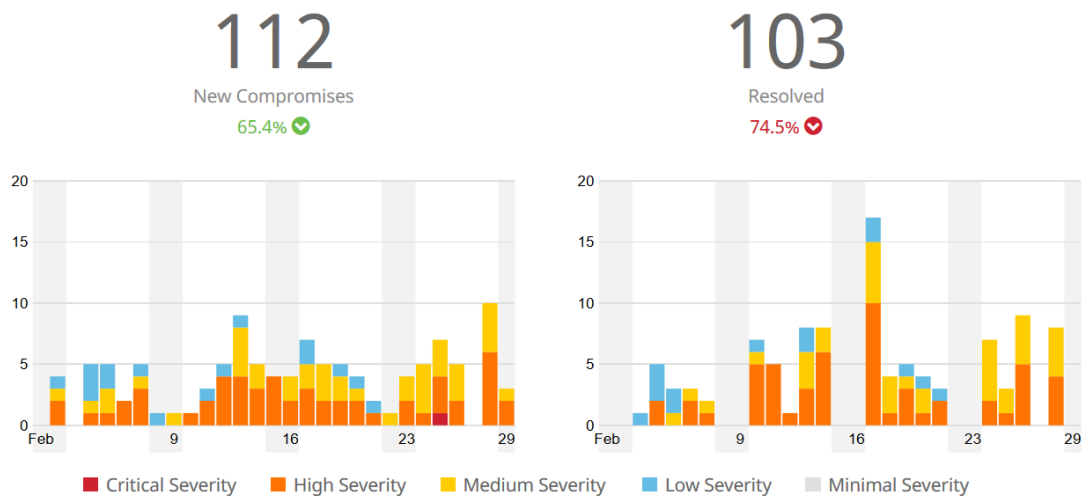
Application	Version	Threats Introduced	Computers Affected	%
● firefox.exe	72.0.2.7321	220	1	18.98%
● chrome.exe	79.0.3945...	76	7	6.56%
● ServiceShell.exe	1.3.0.55	53	6	4.57%
● svchost.exe	6.2.18362.1	50	3	4.31%
● ServiceShell.exe	1.2.0.10	27	1	2.33%
● (other)				63.25%



Number of New Compromises Reported in AMP / Compromises Resolved – February 2020

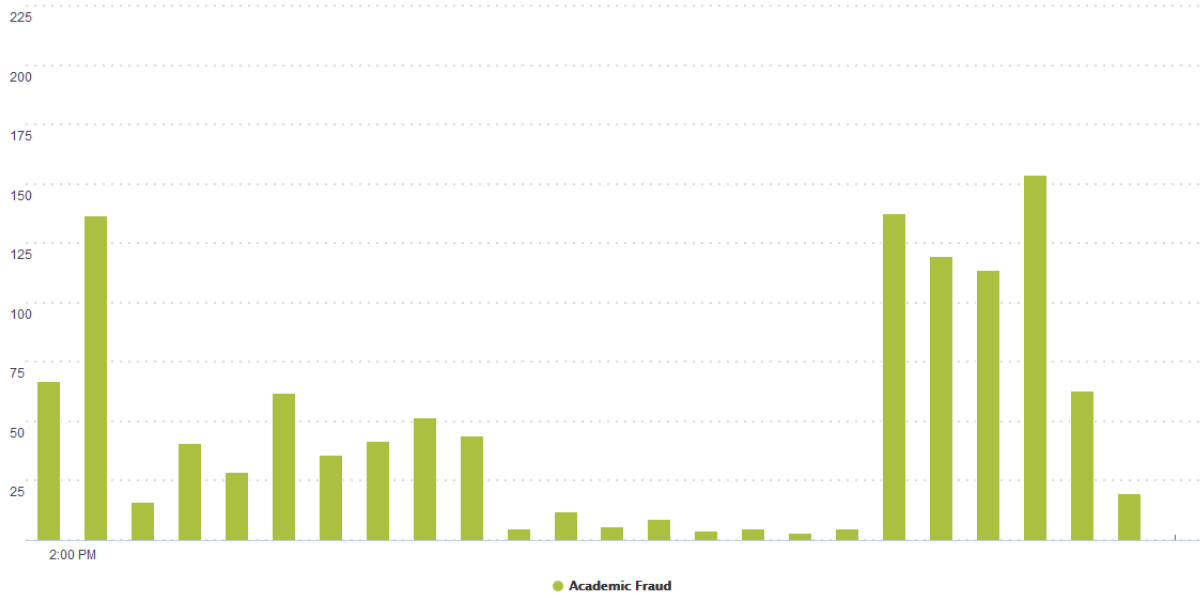
Compromises

Compromises are malicious activity detected by AMP that has not been quarantined and requires additional action. The charts show the total number of new compromises and the number of resolved compromises per day, color-coded by severity.



Web Activity Detected as Academic Fraud Umbrella / OpenDNS – February 2020

Once again, of interest is the number of instances detected by Umbrella as potential academic fraud.

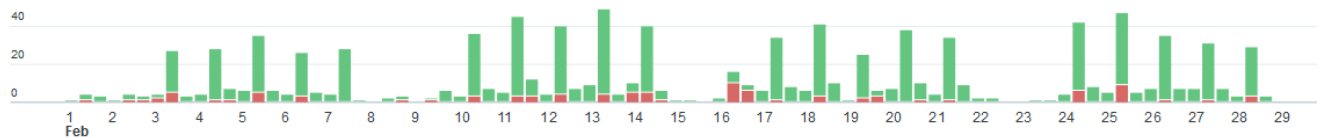


DUO Activity – February 2020

There were 1008 DUO authentication attempts in February 2020 with an 94% success rate. Unsuccessful attempts can be due to user cancellation, wrong code or failure to click to authorize a DUO Push. Failure to authenticate can also result from not having security features, such as screen lock, enabled on the cell phone used to receive DUO pushes or texts.

1k Authentications

Shown at every 8 hours.



Green denotes a successful authentication attempt and red denotes an authentication attempt failure.