Saluki Tech News

Mobile Dawg's Growing Success

The Mobile Dawg initiative is now in its second academic year of operation and the program has had a positive effect on recruitment, student success and retention. The data from recently conducted surveys clearly show that the Mobile Dawg program is helping to attract students and that those students are heavily using the tablets for their coursework, which is resulting in improved student success and higher retention.

Information Technology's survey of the current freshman class concerning the Mobile Dawg project shows that of the students who took the survey, 31% of respondents indicated that the tablet program was a factor in their decision to attend SIU (5.38% of those students listed the tablet program as a major factor in their selection of SIU).

The survey also shows that students are using the tablets in the following ways:
- 75% access electronic textbooks and labs.
- 77% use them for homework.
- 61% watch videos/listen to music.
- 47% use social media.
- 33% use to take notes.
- 25% use to play games.

The Pearson Mobile Device Survey for 2014 (conducted by Harris Poll) shows that:
- 81% of college students agree that tablets will transform the way college students learn.
- 74% of college students believe tablets make learning more fun.
- 66% of college students believe tablets help students learn more efficiently.
- 62% of college students believe that tablets help students perform better in class.

Network usage of Mobile Dawg tablets on the wireless network by freshman based on a four week period in August and September shows that:
- The tablets were logged onto the network for almost exactly one million total hours (59,676,371 minutes) over the four week sample period.
- This is an average of 248,651.54 hours per week.
- This is an average of 35,521.65 hours per day.
- Each device was logged on to the network an average of 5.5 times a day.
- Usage on the rest of campus is much more frequent than usage in the residence halls (approximately twice as much usage on the "campus network" with 336,007 logins compared to 171,698 logins in the residence halls).
- Logins during the week are much more frequent than on the weekend. An average weekday had 23,730 logins while the average weekend day had 4,395 logins.

The student survey cited above indicates that the Mobile Dawg project has had a major impact on the recruitment of first time college students. This data supports the anecdotal evidence at open houses and new student orientations where Mobile Dawg staff are often told something to the effect of "I was on the fence between here and _________ University and decided to come here because of the tablet program."

In addition, SIU's freshman retention was up 3.6% from fall to spring semesters last academic year. Retention of freshman to sophomore students was up 8.3% for fall 2014. Teresa Farnum, retention consultant, noted, "A factor in the increase in retention is likely digital textbooks, technology, WiFi and the tablet initiative. Evidence of this is the 12.5 percentage point increase in the retention of underprepared students. This improvement cannot be attributed to higher profile students; the fact is that these students, whose low ACT scores correlate nationally with a low socioeconomic status, typically struggle to purchase textbooks, and too frequently do not have them—a factor in student learning and success—and students had them this year."

This academic year will prove to be even more successful due to the following factors:
- A new Faculty Technology Mentoring Program that encourages and trains faculty members in the use of the technology for the classroom.
- The tablet devices this year are much more robust (twice as fast) and powerful than the units from last year.
- Keyboards were provided with the tablets this year because many of the electronic textbooks were not written for a touch interface.

Information Technology Notes

Safe Handling of Information Standard

A new standard for the safe handling of sensitive information is in effect for all faculty and staff and will be implemented over time with the assistance of departmental Local Area Network (LAN) Administrators. In some cases, but only under isolated circumstances, student workers may also be affected.

The new standard is driven in large part by a recent audit review, as well as the desire and necessity to protect sensitive, or confidential, information by campus constituents. Sensitive, or confidential, information is defined as "highly restricted" under the SIU Carbondale Data Classification Policy. Examples of "highly restricted" data include: Payment Card Industry (PCI) data including credit card information. Health Insurance Portability and Accountability Act (HIPAA) data that refers to medical-related information. Personal Information Protection Act (PIPA) data, including Social Security number, driver's license or state identification card numbers and credit card or debit card account numbers.

The standard essentially requires all users of "highly restricted" data to take proper precautions when protecting data in electronic or paper form. Requirements include encryption techniques for electronic data at rest and in transit, as well as proper security procedures for paper documents including lockable offices and filing cabinets, redaction and disposal (shredding) of information when no longer needed. Authority for this standard is granted by the SIU Board of Trustees policy, SIU System Information Security Plan, and the SIU Carbondale Information Security Program, or ISP.

The new standard is available at http://oit.siu.edu/_common/documents/Safe%20Handling%20of%20Sensitive%20Information%20Standard.pdf. It is a joint effort between Information Technology and Library Affairs. Direct questions to the information security team at security@siu.edu.

Computer Security and Social Engineering Attacks

Information Security is providing an in-depth look into social engineering – what it is and how to detect, stop and prevent these attacks from occurring. Additional information from the November 2014 Security Awareness Newsletter for Computer Users (SANS) "Ouch!" is available at http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_en.pdf. For more information, email security@siu.edu.

Wireless Scam Warning

There are two active phone scams targeting mobile phones. The first is affecting customers in Illinois. The second has been reported in other states.

The first scam starts with a phone call that appears on caller ID as "Technical Support 1-800-922-0204," which is also the actual number for Verizon Wireless Customer Support. The call plays a recording that asks Verizon subscribers to visit a verizon54 website in order to claim a $54 bonus. When users visit the site, they are asked to log in using their credentials for their Verizon Wireless account. At this point, the site steals the associated usernames and passwords. Anyone who gets a call like this should ignore it. Verizon customers should never use their Verizon username and password to log into any website other than http://www.verizonwireless.com.

The second scam has been reported in Washington, Florida, Georgia, and Massachusetts. The caller states that the Washington State Department of Corrections has issued a warrant for the person receiving the phone call, and that they will go to jail if they don't call the number provided. When the person receiving the phone call returns the call they are informed they owe money and if not paid by the end of the day they will be put in jail. Persons who receive calls such as these or any other scam activities need to be advised to contact their local law enforcement.

UPS Virus

A common scam around the holidays, the UPS virus lures people into opening an attachment that launches a virus. UPS (FedEx and other delivery services have also been the source of scam email) does not request personal or financial information in this way. Report suspicious email and always use the toll-free number or tracking to check on deliveries. Find out more at http://www.snopes.com/computer/virus/ups.asp.