What’s happening on campus?

The Year 2016 in Review

This year we made some more progress towards achieving compliance as a campus. We have convinced two of our vendors of point of sale software to integrate with Bluefin Payment Systems. These integrations are well underway or nearing completion. When finished, the campus merchants using those software applications will have PCI validated point to point encryption. (P2PE) Other campus merchants are seeking to make a change to new software in order to enhance the way they do business. As they seek their new point of sale applications, they do so with P2PE as one of the requirements that the successful vendor must provide.

This is where we currently stand:

- 99% of all revenue from payment cards is taken in a PCI DSS compliant manner.
- 17 out of 21 merchant ID’s are already PCI compliant.
- 2 of the non-compliant MID’s have a software integration underway with Bluefin’s P2PE.
- Three campus merchants (including the other non-compliant areas) are seeking some type of software change.
- The availability of POS software that is already integrated with a P2PE solution has increased significantly.
- 32 regular employees and 13 student interns failed to complete compliance training this year. Some changes will be made in 2017 to rectify this situation.

Did you know?

Earlier this year, following multiple reports of card fraud after payment cards were legitimately used at their restaurants, Wendy’s food chain uncovered malicious software on point-of-sale systems at approximately 300 of their locations. While BU does not have a Wendy’s on campus, many other colleges and universities do. Also, if it can happen to Wendy’s, then it can happen to Einstein Bros Bagels, Tully’s, etc. We are responsible for confirming the PCI Compliance status of those companies we choose to do business with.
2016 Compliance Issues

1. Annual Training - 32 employees never completed the training. Reminders will go out more frequently next year and supervisors will be notified. The module will return to the WeComply web site for all full time employees.

2. Almost no department turned in an AOC in 2016. Remember, an AOC is needed from your third party vendor UNLESS that company appears on the Visa Global Registry of Service Providers. In that case, please take a screen shot of the listing from the Visa web site and place it in your department’s folder on the shared drive.

If you have questions, please contact Steve Duseau. sduseau@binghamton.edu

What the Yahoo Breach Means for Your Institution by CampusGuard

10 Steps to Take with Your Staff

This week Yahoo revealed that thieves stole data on more than one billion user accounts. It was not that long ago that Yahoo warned of a network security breach affecting 500 million account holders. Most likely, at least some or even many of your institution's employees have personal Yahoo accounts that have been compromised. Because the information stolen includes names, e-mail addresses, dates of birth, hashed passwords, and even security questions and answers, we recommend you alert your staff and have them take the following steps:

1) Change Yahoo account passwords and enable two-factor verification.
2) Update passwords on any other accounts if the same password as the Yahoo account was used and always create separate unique passwords in the future!
3) Update security questions and answers if similar information was used for other accounts.
4) Monitor all accounts for suspicious activities.
5) Verify anti-virus software is installed and updated on all personal and work devices.
6) If employees signed up for any services or accounts using a Yahoo e-mail address, update account information immediately and be on the lookout for suspicious activities.
7) Remind staff to be vigilant about potential phishing and malware attacks; after this breach there may be an increase in fraudulent e-mail scams.
8) If employees were using their Yahoo password to access any critical devices or organizational systems, you will want to know so you can update access credentials and monitor activity logs.
9) If employees had any sensitive organizational information in their Yahoo inboxes, have them tell you now so you can formulate an appropriate response strategy.
10) Remind them of your incident reporting procedures - do they know where to report suspicious activities, account passwords changed without permission, inability to access accounts, etc.?

Basic e-mail and information security best practices apply here, and this breach is just another reminder of how important ongoing end-user training and awareness is.