What’s happening on campus?

Next CampusGuard Visit Scheduled

Ed Ko, our QSA from CampusGuard, will visit campus beginning on Wednesday, January 31st through Friday, February 2nd. Currently, the plan is for Ed to visit all merchant departments to assess PCI compliance. Our expectation is for the entire campus to be deemed compliant with the DSS thanks to the scope reduction achieved through the use of P2PE. I will be reaching out to each department to set up a specific day and time for Ed and I to meet with you.

PCI Compliance Training 2018

Regardless of the success of our CampusGuard assessment in early February, PCI Compliance is only achieved when all employees within the CDE complete the annual training requirement. For the approximately 210 employees assigned this training module each year, we expect the UCTD to release the module over the upcoming winter break in late December along with the other required compliance modules. Please take advantage of the offer to save a half day of vacation time by completing all compliance training over the holiday break.

P2PE Solution Progress

The success of our upcoming CampusGuard assessment depends upon the completion of P2PE installations in those areas previously identified. Thus far we have accomplished the following:

- **Events Center:** At our request, Bluefin P2PE was integrated with Agile Ticketing software and implemented at the EC Ticket Office.
- **New Student Programs:** The Bluefin solution was also integrated, again at our request, with VisualZen software and is used at Orientation.
- **Campus Recreation:** We utilized an existing integration between FreedomPay’s P2PE solution and Fusion software which is now in use at the East Gym.
- **Anderson Center:** When Patron Manager software is installed next month, it comes with the Bluefin solution already installed.

This leaves the “pay-in-lane” pay stations at both the parking garage and paid lot as the final places to implement P2PE. This project is in process now.

Did you know?

Data that is not needed should never be stored. However, sometimes there is a legitimate business need to store cardholder data (CHD). Once that data is no longer needed, the PCI DSS includes specific requirements for disposing of CHD whether stored on paper or electronic media.

Remember to get an Attestation of Compliance (AoC) from your third party vendor every year OR a screen shot of that vendor’s listing on the Visa Global Registry. Then put it in your shared PCI folder.
Phishing Biggest Threat to Google Account Security by Michael Mimoso

I. Annual Training - Out of approximately 230 employees, only 4 have not completed the training. Thank you very much to those who have. For BU to achieve compliance in 2018, we need everyone to participate.

II. An Attestation of Compliance (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. Thus far, only Student Accounts, the Fleishman Center, and the Graduate School has provided the proper document. If you need to know which document is needed, check the last newsletter or ask Steve Duseau. **Again, to achieve compliance we MUST have these REQUIRED documents from third parties.**

Google and researchers from the University of California Berkeley attempted to ease some of that pain, and teamed up to analyze how cybercriminals operating underground markets for stolen credentials steal, use and monetize this data. Looking at black market activity from March 2016 to March 2017 and its impact on exclusively Google accounts, the researchers said they wanted to know how the multitude of keyloggers, phishing kits and available data from publicly known breaches for sale can be turned around to learn valid email credentials and in turn control over a user’s online identity.

The news isn’t good.

In a paper presented at the recent Conference on Computer and Communications Security, Google said that between 7 percent and 25 percent of exposed passwords matched a victim’s Google account. Overall, Google and UC Berkeley estimates there are 1.9 billion usernames and passwords cultivated from breaches that are being traded on the black market. Tack on to that another 12.4 million victims of phishing kits and another 788,000 victims of commercial keyloggers and the climate is dire.

“We observe a remarkable lack of external pressure on bad actors, with phishing kit playbooks and keylogger capabilities remaining largely unchanged since the mid-2000s,” the researchers wrote.

Of the black markets tracked in this research, Google said there are 25,000 tools for phishing and keyloggers at attackers’ disposal. Even though attackers are failing to access Google accounts three out of four times, it’s not for a lack of effort.

“Because a password alone is rarely sufficient for gaining access to a Google account, increasingly sophisticated attackers also try to collect sensitive data that we may request when verifying an account holder’s identity,” Google said in a blog post accompanying the report. “We found 82 percent of blackhat phishing tools and 74 percent of keyloggers attempted to collect a user’s IP address and location, while another 18 percent of tools collected phone numbers and device make and model.

“By ranking the relative risk to users, we found that phishing posed the greatest threat, followed by keyloggers, and finally third-party breaches,” Google said.

Phishing remains one of the most successful phenomena in security, despite more than a decade of education and examples of successful attacks based on the technique.

“Hijackers also have varying success at emulating the historical login behavior and device profile of targeted accounts. We find victims of phishing are 400x more likely to be successfully hijacked compared to a random Google user,” the researchers wrote. “In comparison, this rate falls to 10x for data breach victims and roughly 40x for keylogger victims. This discrepancy results from phishing kits actively stealing risk profile information to impersonate a victim, with 83 percent of phishing kits collecting geolocations, 18 percent phone numbers, and 16 percent User-Agent data.”

Backing this up, the researchers found more than 4,000 phishing kits used in active attacks during the period of time studied compared to 52 keyloggers. Phishing kits are packages of all-in-one tools for creating and configuring content used in these attacks, including email and website creation. These kits generally are used to collect a victim’s username and password, but also geolocation information and a lot more. The credentials are forwarded to the attacker over SMPT, FTP or uploading them to a website. Most phishing kits—and keyloggers—are configured to steal Gmail credentials, the study said. Yahoo webmail users, however, were the biggest victims of credential leaks. Yahoo has reported that at one time all of its 3 billion users’ data has been exposed to attackers.

Google said it has already used this data to reinforce the security of Gmail.

“Our findings illustrate the global reach of the underground economy surrounding credential theft and the need to educate users about password managers and unphishable two-factor authentication as a potential solution,” the researchers wrote.