Thanks to everyone who participated in our payment card terminal security forum.

Please share the session recording with those who missed,

https://web.microsoftstream.com/video/c7002670-79a6-4f66-bb08-375e95d0a3a0

Lighting could be better and it is an hour long with some post presentation Q&A so here are the highlights:

**Mike Syljuuberget Head Cashier BAO 6-3164**

1. Go to person for card processing equipment and support
2. Check with Mike before allowing anyone access to your terminals for “maintenance or critical updates”.
3. Ensure terminals are configured to settle automatically every night to secure funds, wipe cached card data and avoid higher card processing fees.
4. Deposit credit card proceeds weekly in the same month to make bank reconciliation easier.
5. Don’t retain full card numbers for refunds. Call Cashiers to obtain original card number for any refunds.
6. When calling the Elavon number on the terminal for support you will be asked for identifying info. Provide merchant ID number, department name, and last batch amount.

Jarvis Gilmore Qualified Security Assessor Campus Guard
1. All terminals accept chip cards and the cards should always be inserted (or dipped). Otherwise liability for reported fraudulent use shifts to merchant. Watch for chip cards that fail when inserted three times they may be counterfeit with non-functioning chip but good magnetic stripe.
2. All terminals also accept NFC (Near Field Communication) smart phone contactless transactions (Apple Google and Samsung Pay)
3. All terminals, (except Ticketmaster) now accept American Express.
4. No-one on campus is processing chip and PIN. International credit cards and a few US ones will require a PIN for credit transactions. Can turn device around toward customer or order PIN Pad if volumes increase.
5. Payment Card Acceptance Policy is in the UO Policy Library.
6. Payment Card Acceptance Procedures are on the Business Affairs site including merchant responsibilities, sample operating procedures, incident response plan. You will have to log in using Duck ID.
7. Devices plugged into the network require SAQ B-IP, firewall, vulnerability scanning and segmentation testing. They must be tagged by IT staff.
8. Most UO terminals have PTS 3 encryption and PCI Council approval for PTS 3 expires April 30 2020. We can continue to use them. When we do replace them we should replace them with terminals with highest possible certification level (PTS 5). If cellular look for 4G and 5G network support.
9. Card skimmers are used to steal card data. These devices can be installed over card readers in seconds and are hard to identify unless you are familiar with, and routinely inspect your device. Chip card skimmers also exist.
10. Merchant departments should have an inventory of terminals that includes serial number, make model physical location and photo.
11. UO does not allow use of Square because they shift breach liability in their contract to the merchant and require that funds be deposited to their bank. Transaction volume is also limited.
13. Do not honor card information provided by email. Delete the message and ask the customer to provide number over the phone using voice. In future, email may be filtered to prevent card data.
14. Never store full card numbers in a computer file (Word, Excel, etc.).
15. Never send full card numbers in a text message.
16. When accepting online payments (ecommerce) on site at an event, avoid using a UO computer, computer lab or kiosk, and instead assist the customer in using their personal device.
17. Avoid storing full card numbers (and especially the card verification code) on paper. If you do have paper records, for pre-orders for example, lock it up, redact or confidentially recycle as soon as processed and no longer needed. Maximum retention is 1 year. Don’t send in campus mail. Approval number, last 4, name and amount can be retained longer.
18. Card acceptance over the phone brings the university voice over IP VOIP network into scope for PCI DSS. The security team needs to ensure those packets are encrypted in transit. Analog lines are actually more of risk of tapping. If phone calls are recorded (Advancement Call Center Ruffalo Cody) that data is also in scope. Best if Ruffalo is phone provider.
19. Data breaches are expensive, bank can pass on card brand fines, we must notify customers, must conduct forensic investigations, must conduct QSA audits for compliance annually.
20. Nebraska book company had two card data breaches this year.
21. Card Data Security should be ‘business as usual’, daily terminal inspections, inventory, not just the annual self-assessment and training.
22. Cellular terminals support 3G network. May have to replace when switch to 4G.
23. I will put this short and scary skimming video in the annual PCI training.

Thanks again.

Mark McCulloch
Director Info Systems Business Affairs
University of Oregon
541 346-6249
Hello everyone,

This is a reminder to encourage supervisors and staff engaged in credit card processing using payment card terminals to participate in the security discussion tomorrow afternoon at 2PM in 115 Lawrence Hall. IT support staff are also encouraged to participate.

See you tomorrow.

Agenda below.

Thanks

Mark

---

From: Mark McCulloch
Sent: Monday, May 20, 2019 2:46 PM
To: Mary Ellen Mansfield; Sherri Nelson; Chris Krabel; Volga Koval; Angie Peatow; Cleven Mmari; Gregg Wendland; David Reesor; Krista Borg; Andre Le Duc; Jamie Leaf; Trish Mace; Paul Katz; Karen Jefferis; Cleven Mmari; Stephen Stolp; John Sargeant; Laura Jorgensen; Kari Vanorsdel; Shirley Brabham; Jessica Carlson; Diertra Lomeli; Lalla Pudewell; Laura McCoid; Mike Ruell; Corie Shupe; Skip McFarlane; Sandy Cummings; Carrie Toth; Robynn Medew; Karen Schneider; Brian Lee
Cc: Kelly Wolf; Jose Dominguez; Leo Howell; Matt Love; Michael Syljuuberget; Krista Borg
Subject: Re: Payment Card Terminal Security Forum Wed May 29th 2PM

Campus merchants,
The payment card terminal security forum will take place Wednesday May 29 2PM to 3:30 PM in 115 Lawrence Hall

Agenda:

Welcome and introduction  Mark McCulloch Director Information Systems Business Affairs (10 Minutes)

Batch Settlement and Deposits  Mike Syljuberget University Cashier (10 minutes)

Security Requirements Discussion  Jarvis Gilmore QSA Campus Guard (60 minutes)

All terminals:
4.2 Policy regarding email
7.1 Access to system and cardholder data limited
9.5-9.8 Physical security of any media containing card holder data (written procedures)
9.9.1 Device inventory
9.9.2 Device inspection (written procedure)
9.9.3 Staff training to detect and report tampering/replacement
12.1 Security policy
12.6 Security awareness training
12.8 Service provider procedures
12.10 Incident response plan

Ethernet connected terminals:
1.1-1.2 Network diagram and firewall configuration
11.2 Quarterly external scans
11.3 Segmentation and penetration testing

Final Questions and Closing Remarks  Mark McCulloch Director Information Systems Business Affairs (10 minutes)
Please encourage managers and staff in your unit who are engaged in card acceptance using terminals to register and participate. This session will be recorded for those who are unable to participate in person. Participation in person, or by viewing the recording, fulfills the annual security awareness training requirement for the March 2020 PCI self-assessment.

Please let me know if you have any questions or suggestions.

Thanks

Mark McCulloch
Director Info Systems Business Affairs
University of Oregon
541 346-6249

From: Mark McCulloch <MMcCullo@uoregon.edu>
Sent: Wednesday, May 15, 2019 12:47 PM
To: Mary Ellen Mansfield <mem@uoregon.edu>; Sherri Nelson <sherrin@uoregon.edu>; Chris Krabiel <ckrabiel@uoregon.edu>; Volga Koval <koval@uoregon.edu>; Angie Peatow <peatow@uoregon.edu>; Cleven Mmari <cmmari@uoregon.edu>; Gregg Wendland <gwendla@uoregon.edu>; David Reesor <dreesor@uoregon.edu>; Krista Borg <KBorg@uoregon.edu>; Andre Le Duc <leduc@uoregon.edu>; Jamie Leaf <leaf@uoregon.edu>; Trish Mace <tmace@uoregon.edu>; Paul Katz <pdkatz@uoregon.edu>; Karen Jefferis <karensj@uoregon.edu>; Cleven Mmari <cmmari@uoregon.edu>; Stephen Stolp <stolp@uoregon.edu>; John Sargeant <sargeant@uoregon.edu>; Laura Jorgensen <laj@uoregon.edu>; Kari Vanorsdel <kvorsdel@uoregon.edu>; Shirley Brabham <shirleyb@uoregon.edu>; Jessica Carlson <carlsonj@uoregon.edu>; Diertra Lomeli <dlomeli@uoregon.edu>; Lalla Pudewell <pudewell@uoregon.edu>; Laura McCoid <lmccoid@uoregon.edu>; Mike Ruell <michaelr@uoregon.edu>; Corie Shupe <cfshupe@uoregon.edu>; Skip McFarlane <skipmcf@uoregon.edu>; Mckenzie Winders <mwinders@uoregon.edu>; Charles Hollands <hollands@uoregon.edu>; Kaira Chandler <kaira@uoregon.edu>; Alex Cardinaux <acardinx@uoregon.edu>; Peggy Schneider <pwebb@uoregon.edu>; Tawnee Gerig-Brunson <tbrunson@uoregon.edu>; John Ivie Jr <iei@uoregon.edu>; Sandy Cummings <sandyc@uoregon.edu>; Amanda Smith <asmith@uoregon.edu>; Robynn Medew <rmedew@uoregon.edu>; Karen Schneider <karens55@uoregon.edu>; Brian Lee <blee@uoregon.edu>
Subject: Payment Card Terminal Security Requirements Forum Wed May 29th 2PM

Hello campus merchants,

Our security assessor Jarvis Gilmore, our IS security team, and I will host a forum to discuss security requirements for in person/mail/fax/telephone credit card transactions on Wednesday May 29th from 2 to 3:30 in 115 Lawrence Hall.

All employees who operate payment card terminals, their supervisors and IT support staff are invited to participate.
Please mark your calendars.

An agenda and registration survey will be circulated shortly.

Please share this announcement with others I may have omitted.

This session will be recorded for those who are unable to attend in person.

We look forward to seeing you.

Please let me know if you have any questions.

Thanks

Mark McCulloch
Director Info Systems Business Affairs
University of Oregon
541 346-6249