Payment Cards Processing at UNL

VOLUME 10, ISSUE 2 APRIL, 2016

University of Nebraska —Lincoln
PCI Compliance Task Force

Annual Training Requirements for Card Handling

All parties handling cardholder data must adhere to specific training requirements in PCI V3.1. Since only your department knows which individuals are involved in card processing, the monitoring of this training is the department's responsibility.

Cash Handling Training

All personnel connected in any way with cash handling, including payment card transactions, must review cash handling policies & procedures on a regular basis. A review should occur at least annually and documentation of this review should be retained within the department. The Cash Handling Policies & Procedures training is available at: http://bursar.unl.edu/cash-handling-policies-procedures

Security Awareness Training –Requirement 12.6

All personnel connected in any way with cardholder data need to annually complete security awareness training at http://its.unl.edu/security/security-awareness-training.

Departments can contact Cheryl O'Dell with a listing of employees who need to complete the training if you'd like to request access for several instead of individual requests. Cheryl can also provide reporting so departments can ensure all employees have complied with this requirement.

Device Tampering Training –Requirement 9.9

All personnel must be trained to protect devices which capture payment card data through physical interaction (i.e. swipe, dip, or wave) with a payment card. Personnel must be trained to be aware of attempted tampering or replacement of devices, and terminals must periodically be inspected to look for tampering and substitution.

Two resources that we've found to be helpful are:

- https://www.pcisecuritystandards.org/documents/Skimming%20Prevention%20BP%20for%20Merchants%20Sept2014.pdf
- https://usa.visa.com/dam/VCOM/download/merchants/data-security-protect-terminals-from-illegal-tampering-020513.pdf

Either of these could be used for training within departments and, again, the department must document all who need training have received it.

Conversion from TSYS to Elavon is Nearing Completion

We are excited to have 43 merchant accounts active under Elavon. We have another 18 in the process of converting. This leaves just 4 more MIDs to go.

We understand the conversion has been a very time-consuming process for all involved. We've appreciated everyone's patience and understanding throughout. We hope to be completely converted very soon.

Skimming Devices

Take a look at these YouTube videos showing a criminal placing a skimmer over a terminal. It's that easy!

https://youtu.be/y83ZgzuFBSE

https://www.youtube.com/watch?v=gJo9PfsplsY

University of Nebraska —Lincoln
PCI Compliance Task Force

Information Technology Services (ITS)
Cheryl O'Dell cherylo@unl.edu
Dan Buser dan.buser@unl.edu

Office of the Bursar
Lyda Snodgrass lsnodgrass1@unl.edu
Jennifer Hellwege jhellwege@unl.edu

The PCI Compliance Task Force is a collaboration between Information Technology Services (ITS) and the Office of the Bursar. It is a cross-functional team responsible for administering the University of Nebraska-Lincoln payment card policies and procedures, monitoring payment card activity, and educating merchants.

Still Experiencing Terminal Issues? Please Report Them

We have a number of merchants whose stand-alone terminals are still experiencing issues. Please continue to report them to the Bursar's Office so we can forward them on to our Implementation Team at Elavon. We understand this is time consuming, but in order for them to be thoroughly addressed, it is necessary. The most common issue is the Comm Error. This seems to be one they just can't get resolved for us. So please continue to let us know when you see it occur. We will continue to work with Elavon until all terminals are working properly.

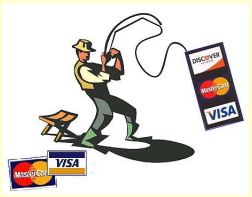
Update IPs for QualysGuard Scans

Dan Buser maintains the IP addresses for the PCI scans. Please contact him if you have any updates to your IPs or to confirm what is currently being scanned for your department's merchant account(s).

Be Aware of Phishing Attempts

Phishing attempts seem to be on the rise everywhere. Do not click on any links that appear in emails unless you are certain the sender is legitimate. Here's some great information on what to look for and how to report any incidents you see.

http://news.unl.edu/newsrooms/unltoday/article/awareness-caution-key-to-avoid-phishing-scams/



Merchant Connect Inactivity Will Cause Account to be Locked

We've had a few Merchant Connect users get locked out of their accounts for inactivity. Per Elavon, your account is locked after 90 days of inactivity. If you are locked out, proceed with "forgot password?" on the login page for assistance.

Use Firefox to View Monthly Statement in Merchant Connect

This past month, a user discovered Internet Explorer does not work to view your Monthly Statement in Merchant Connect. The result was gibberish. Firefox is able to view the statement without issue.