Payment Cards Processing at UNL

VOLUME 7, ISSUE 3 AUGUST, 2013

University of Nebraska —Lincoln
Bursar's Office

PCI DSS Version 3.0 to be Released Soon

The PCI Security Standards Council recently released the document, "PCI Data Security Standard and Payment Application Data Security Standard Version 3.0 Change Highlights". This document is available at the PCI website:

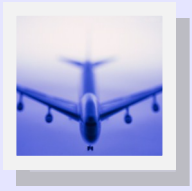
https://www.pcisecuritystandards.org/security_standards/documents.php

According to the document, Version 3.0 will be introduced in November 2013. UNL's 2013-14 PCI Compliance should still fall under Version 2.0, but TSYS Merchant Solutions will have to confirm that. Nevertheless, we need to be thinking ahead and preparing for the new requirements. Some of the notable items:

- Requirement 1—Have a current diagram that shows cardholder data flows.
- Requirement 2—Maintain an inventory of system components in scope for PCI DSS.
- Requirement 9—Protect POS terminals and devices from tampering or substitution.
- Requirement 12—Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity. Service providers to acknowledge responsibility for maintaining applicable PCI DSS requirements.

Once Version 3.0 is released, we will have much more information, but for now it's just good to have an idea of what is to come in our ever changing world of PCI.

Welcome to Education Abroad our newest payment card merchant!



2012-13 PCI Compliance Documentation is Complete

Our PCI documentation has been submitted to TSYS Merchant Solutions for another year. Thank you for all your efforts in getting this done. It is a significant achievement, and you all contribute greatly to its completion.

Correction: "Fastpay/Quick Payment Service" Article

Included in the May 2013 newsletter was an article highlighting the Fastpay/Quick Payment Service programming option. We have since learned this programming prints both a customer and sales receipt. Neither copy includes a line for the customer's signature. We had previously understood that only a customer copy printed. We apologize for this incorrect information.

RFP In Process for Credit Card Payment Services

The State of Nebraska released a Request for Proposal (RFP) on June 3, 2013. The RFP was for ACH Origination Services and Credit Card Processing Services. Being under the State's umbrella, this RFP includes the University's credit card processing services as well. Proposals were opened August 5th and are currently under review. Lyda Snodgrass, UNL Bursar, is on the review team and will be representing UNL's interests throughout this process.

The contract awarded from the RFP will be for credit card processing services starting July 1, 2014. What does this mean to us? Our Acquirer, TSYS Merchant Solutions, could be changing.

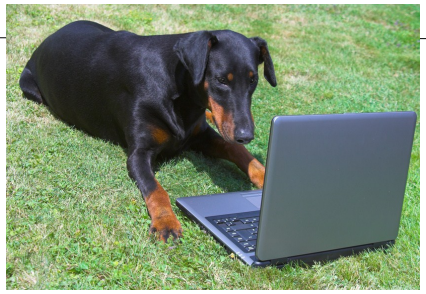
University of Nebraska —Lincoln
Bursar's Office

121 Canfield Administration Bldg
Lincoln, NE 68588-0412

Phone: 402-472-1734
Fax: 402-472-2959
E-mail: bursar@unlnotes.unl.edu

The Office of the Bursar is responsible for administering the University of Nebraska-Lincoln money handling policies and procedures. Don't ever hesitate to contact us with any receipting questions you may have.

Security Threats Not Wavering



Security continues to be a challenge for everyone. No matter if you are in the US or overseas. No matter if you are a small retailer that processes cards solely via a phone terminal or a large university that processes cards online and via phone terminals for a wide variety of activities. No one is immune to breaches and in spite of the humor behind this picture, we really do need to be a constant watch dog to our systems and procedures to ensure we always have security in mind in all that we do. Trustwave recently published their Executive Summary: 2013 Global Security Report Preview. Here are some of the highlights from that document:

Some Key Discoveries from 2012:

- **Retail businesses** are back in the crosshairs. The retail industry made up **45% of investigations**—the highest of all sectors.
- **Web applications** have emerged as the **#1 targeted attack vector**.
- **Mobile malware exploded by 400%**.
- Spam volume has declined, but its impact has not. Even though spam volume in 2012 shrank to a level that was lower than it was in 2007, spam still represents an astounding 75.2% of a typical organization's inbound email. Research has found that **10% of spam messages are malicious**.
- Basic security measures are still not in place. **"Password1"** continues to be the most common password used by global businesses. Also **50% of user passwords** analyzed are **using the bare minimum**.

Tactical Threat Intelligence:

- **Encryption Sophistication** - The use of encryption by attackers during data exfiltration is on the rise, **over 25%** of all data was encrypted by cybercriminals
- **Memory Scraping Dominant** - The most popular malware family was memory scraping. 20% of new case samples included memory scraping functionality, and such activity was detected in almost **50% of investigations** where associated malware had identifiable data collection functionality.
- **PDF Files at Risk** - Of all client-side attacks observed, **61% targeted Adobe Reader users** via malicious PDF's.
- **Blackhole on the Rise** - Versions of the **Blackhole exploit kit made up over 70% of all client-side attacks** serving up zero-day exploits.
- **SQL & Remote Still Reign** - Always the two most noteworthy methods of intrusion—**SQL injection and remote access made up 73% of the infiltration methods** used by criminals in 2012.