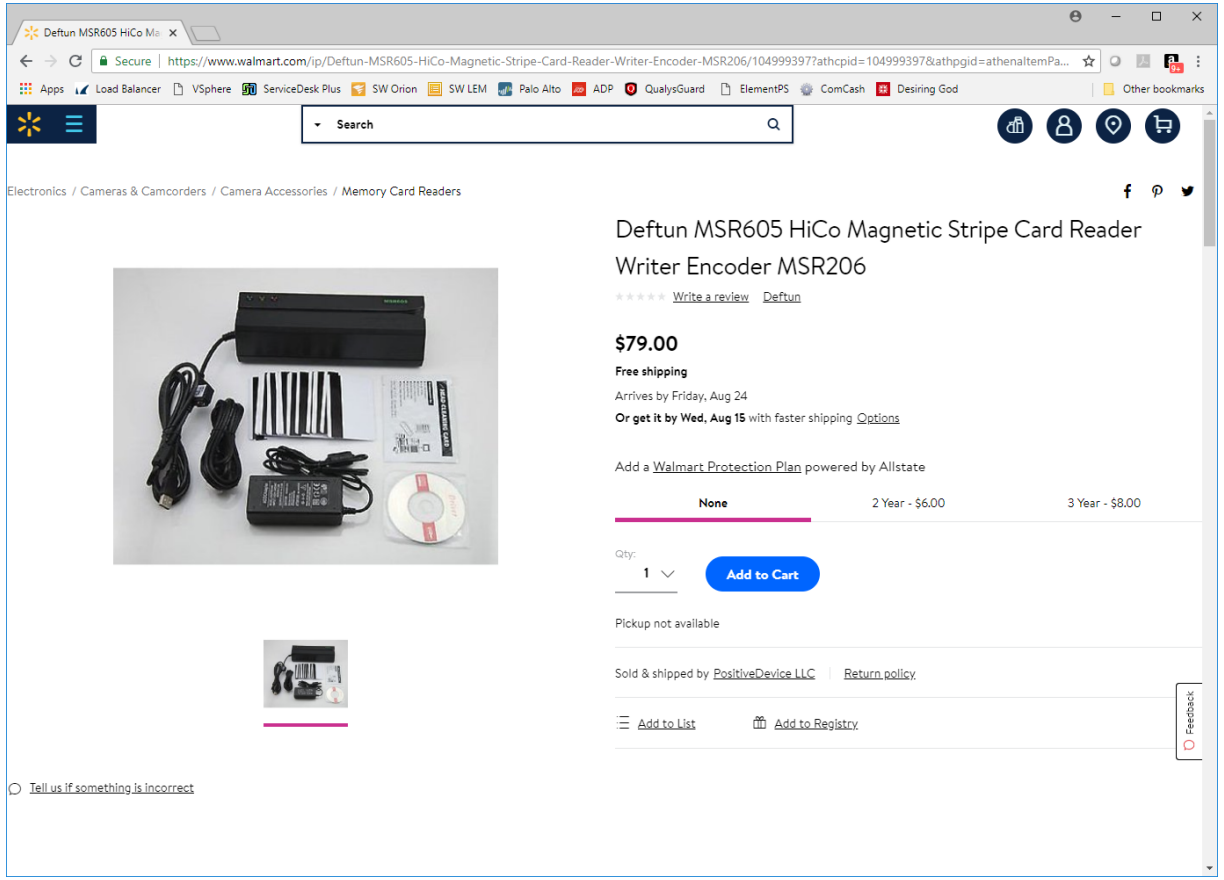

# Cyber Security – PCI Compliance

Chairman's Seminar – Steven Gumerman, Director of IT Infrastructure

# Credit Card Skimmers

# WHY ARE THERE SO MANY?




***MOSTLY, BECAUSE CREDIT CARD THEFT IS EASY***

***ALSO, BECAUSE AS SOON AS THE CARD COMES OUT OF SOMEONE'S WALLET/PURSE, HLSR IS RESPONSIBLE FOR STOLEN INFORMATION.***

# HOW TO IDENTIFY CREDIT CARD SKIMMERS

# Credit Card Data and Cyber Security

# CREDIT CARD PAYMENT POLICY AND GUIDELINES

Acronyms/Definitions:

Payment Card Industry (PCI) and Data Security Standards (DSS).

HLSR undergoes an annual PCI audit to ensure that we are safeguarding ALL credit card data.

Ensuring that Point of Sale (POS) systems are secure is a major component of the audit.

Not passing the audit has an affect on our insurance premiums and our ability to continue processing credit cards.

# WHAT INFORMATION ARE WE CONCERNED ABOUT?

Cardholder Data

- The Credit Card Number
- Name On The Credit Card
- Expiration Date

WE NEVER OBTAIN OR RETAIN THE FOLLOWING!!

- 3 or 4 digit PIN on the Credit Card
- Debit Card PIN

# SAFEGUARDING CARDHOLDER DATA

- If cardholder data is in HLSR's possession, it is HLSR's responsibility to keep it secure.
- It is the responsibility of the business process managers to ensure controls are in place to limit access to the stored files.
- Quarterly, business process managers should monitor office areas to ensure cardholder data is properly secured.

# SAFEGUARDING CARDHOLDER DATA - CONTINUED

- Lock up documents containing cardholder data, both before and after the transaction is processed.
- Process credit card transactions within 24 hours of receiving cardholder data.
- At the end of the retention period, remove cardholder data from the bottom of paper forms and cross-cut shred it.

# SAFEGUARDING CARDHOLDER DATA - CONTINUED

- Advise customers not to communicate cardholder data by email, text or fax.

For those that do anyway:

- Monitor mailbox activity for cardholder data so that no documents are left unprocessed for more than 24 hours.
- Lock your pc when leaving it unattended.
- Delete e-mail messages immediately after the transaction is processed.
- Further delete the e-mail message from the Deleted Items folder.
- If printed, use the same guidelines as for paper forms containing cardholder data.

# SAFEGUARDING CARDHOLDER DATA - CONTINUED

- Do not store cardholder data in spreadsheets, databases, flash drives or any other method that enables the user to distribute or transport data.

- Ensure volunteers are aware of HLSR guidelines.

# CREDIT CARD MACHINES/TERMINALS

- Every operator or supervisor - review the terminal to see if it looks normal. Thieves obtain card data using skimmers.
- Never leave the credit card device unattended.  Lock it up when not in use.
- Keep the credit card in plain sight of the customer.  Preferably, have the cardholder swipe or insert their own card.
- Utilize a log to track the inspection and use of the terminals.

# NEVER DO THE FOLLOWING

- Never acquire or disclose any cardholder data without the cardholder's consent.
- Never collect the 3 or 4 digit code from the card or a PIN from a debit card.
- Never transmit or send cardholder data by e-mail, fax, text or any other end-user messaging technology.
- Never scan or copy any form that includes cardholder data.
- Never leave temporary sensitive information on your desk, screen, vehicle or in any public area.
- Never hold or retain any forms that contains cardholder data for more than 24 hours before submitting them to a designated member of the HLS&R staff.
- Never share a personal account password that has access to HLS&R systems.

# AS CHAIRMAN, YOU WILL DO THE FOLLOWING

- Escort and supervise all visitors including HLS&R personnel in areas where cardholder data is maintained.
- Store all physical documents or storage media containing cardholder data in a locked drawer, locked filing cabinet, or locked office.
- Destroy cardholder data using a cross-cut shredder or with an approved service provider.
- Report immediately a credit card security incident to either the General Counsel or the Chief Technology Officer.
- Keep a log of all credit card devices.
- Place your credit card device in a secure location and periodically inspect the device for tampering.

# E-Mail and Cyber Security

# Accume Partners Phishing Awareness

## What is Phishing?

- Phishing – Cybercriminal attempts to steal personal and financial information or infect computers and other devices with malware and viruses
- Designed to trick you into clicking a link or providing personal or financial information
- Often in the form of emails and websites
- May appear to come from legitimate companies, organizations or known individuals

## Checking for Legitimacy:

- **Check The Address - The email address was from a free email account.**

Thu 2/12/2015 5:42 PM

Jonathan Doe <jdoe.acmebank@gmail.com>

Employee Satisfaction Survey - 2015

- **Check The Link - The link displayed was different than the true link.**

Please take a few mi[illegible] log in, all responses will be aggregated and anonymous.

http://bankbenefits.ddns.net/target.php?id=mstander&anum=6
Click to follow link

https://2015survey.acmebank.com

Thank you,

Note: The true link is different than the advertised link.

## Avoid Being Phished:

| | |
|---|---|
| Who is sending the email? | • Always look at the address to make sure that the email came from:<br>• The person you expected<br>• The domain you expected<br>• Emails that come from @gmail.com, @yahoo.com, @hotmail.com or similar domains should be viewed with suspicion. |
| Where is the link taking you? | • Misspelled domain names are likely to be malicious. Hackers frequently use close misspellings.<br>• Always place your mouse over the link and make sure that the address to which you will be sent is the address that you expect to visit. |
| What are the contents of the email? | • Only open email attachments that you were expecting.<br>• If you are suspicious of the email, don't click the link and don't reply to the email. Use the phone or a new email to contact the alleged sender and make sure the email is legitimate. |
| What do you do if you think you have been phished? | • Never reply to a suspect email. Replying to a malicious email can give hackers a lot of information about you and the technical infrastructure of the organization.<br>• If you think you've been Phished, report it to your IT department immediately. |

## Checking for Legitimacy on Mobile Devices:

- **To see the sender's address, tap on the displayed name. A new screen will open that shows the full email address.**
- **Verify that the sender's address is what you expect.**
- **To check the link, touch and hold the link. A new dialog box will open that shows you the true link.**
- **From the dialog box you can either open the link or cancel the action.**

## Accume Partners Contact Information


*Matthew Bland*
*Network Security Specialist*
*mbland@accumepartners.com*
*Office: 856.914.9500 x309*
*Direct: 281.942.8465*

*Josh Cooper*
*Senior IT Auditor*
*jcooper@accumepartners.com*
*Office: 856.914.9500 x308*
*Direct: 281.942.8296*

# E-MAIL DO'S AND DON'TS

Do's

- Always think before clicking on an e-mail link or attachment.
- Listen to that voice that says "This e-mail seems odd".
- Keep in mind companies are sending fake phishing e-mail to report who does not follow cyber security policies.
- Call or text the sender if an e-mail looks suspicious to verify validity.

Don'ts

- Don't enter your work credentials on a website based on links received through an unsolicited email.
- Don't trust an email from HLSR employees that don't come from the @hlsr.com or @rodeohouston.com domain.
- Don't e-mail the sender if an e-mail looks suspicious to verify validity.


Questions?


LET'S
RODEO
FEB. 27 – MARCH 17, 2024
rodeohouston.com