PCI DSS Security Awareness Training for Credit Card Merchants at

The University of Tennessee

and

The University of Tennessee Foundation

Presented by

UT System Administration
Information Security Office

Agenda

- PCI DSS Overview
- PCI DSS Compliance
- Merchants' Roles & Responsibilities
- Identifying & Reporting Data Breaches
- POS Terminal Fraud & Protection
- Merchants' Annual Obligations

PCI DSS Overview

- PCI DSS is the Payment Card Industry Data Security Standards.
- PCI DSS requirements are applicable to all merchants who process, transmit, or store cardholder data, regardless of the size or number of transactions.
- PCI DSS requirements also apply to all third-party service providers.
- The payment brands (e.g., VISA, MasterCard), as well as the acquiring banks (e.g., Elavon, FirstData) are responsible for enforcing PCI compliance.

PCI DSS Security Training Requirements

- Every person involved in processing cardholder data is required to complete annual PCI DSS security training.
  - This includes all students employed by the merchant, if credit card processing is part of the job.

- This training will help you meet the following requirements:
  - Requirement 9.9.2
  - Requirement 9.9.3
  - Requirement 12.6

Maintaining PCI Compliance

- PCI DSS compliance is not optional!
- Be able to honestly answer “Yes” to each requirement in the SAQ that is appropriate to your merchant processes.
- If you answer “No” for any sub-requirement, you must have a plan of action and date for remediation.
- Follow only those processes for which you have been approved.
- Contact the Treasurer’s Office or the UTSA ISO should you have any questions or concerns about compliance.

The Cost of Non-Compliance

- Suspension of merchant account(s)
- Fines to be paid by the merchant
  - As high as $500,000 per data security incident
  - As high as $50,000 per day for non-compliance with published standards
- All fraud losses incurred from compromised account numbers to be paid by the merchant
  - From the date of the compromise forward
- Cost of re-issuing credit cards to be paid by the merchant

The Cost of Non-Compliance

- Increased transaction fees charged by the bank to be paid by the merchant
- External incident investigation to be paid by the merchant
  - Estimated cost is $30,000 - $300,000 per incident investigation
- Remediation costs to be paid by the merchant
- Legal fees, settlements, and judgments to be paid by the merchant

The Cost of Non-Compliance

- One compromised UT (UTFI) merchant can adversely affect the remaining merchants throughout the entire system.
  - Random external audits by a PCI Security Standards Council-certified assessor for any UT (UTFI) merchant
  - Change in merchant level or SAQ type

- **Remember that the University's and Foundation's reputations are at stake!**
  - Loss of sales and loss of donations as customer confidence declines
  - Possibly a far greater loss than any fines or fees
  - Longer recovery when repairing reputation

PCI Policies

- Read and follow UT's FI0311 – *Credit Card Processing*.
  - Fiscal and IT policies are available on the UT Policy website: http://policy.tennessee.edu
- Maintain and follow internal policies and procedures.
  - Merchant internal documentation templates are available on the PCI Compliance website: http://security.tennessee.edu/pci-dss-compliance-information/.
- Regularly review these policies and standards:
  - IT0110 – *Acceptable Use of Information Technology Resources (AUP)*
  - IT0115 – *Information and Computer System Classification*
  - FI0120 – *Records Management*
  - UT's *PCI DSS Incident Response Plan*

FI0311: Roles & Responsibilities

Merchants (Departments/Units)

- Complete annual SAQ and maintain compliance at all times
  - Notify Treasurer's Office and campus CBO of any proposed change in approved processing
- Maintain internal documented policies and procedures
- Maintain PCI inventory list
- Complete annual PCI security training

FI0311: Roles & Responsibilities

Merchants (Departments/Units)

- Protect cardholder data and ensure appropriate security controls
  - Technical controls on computers that process PCI data
  - Terminal (POS) software is always up-to-date
  - Computers are in the segmented cardholder data environment (SAQs A, A-EP, B, B-IP, C, C-VT, D)
  - Computers/servers serve only one function…PCI
  - Notify campus CIO when there are changes to system resources
- Financially responsible for all costs associated with compliance, including fines, fees, and remediation expenses

Primary Causes of PCI Data Breaches

- **Being non-compliant with the PCI DSS requirements**
- Attacks on users
  - Malware
  - Man-in-the-middle attacks
- Default or guessable passwords
- PCI devices used for non-PCI tasks
- PCI devices using Wi-Fi networks
- Physical tampering of unmanned or unattended POS devices
- Remote access
- Unpatched systems

Detecting a Suspected Data Breach

- Anti-virus programs malfunctions or becomes disabled for no apparent reason
- Excessive failed login attempts
- Unexpected system reboots or shutdowns
- Unexplained user accounts

Detecting a Suspected Data Breach

- Suspicious after-hours activity on PCI devices
- Unexplained modification or deletion of data, such as event logs
- Unknown files, software, and/or devices installed on PCI systems, including archived, compressed, or encrypted files in system directories
- Unknown or unexpected network traffic

PCI Incident Response

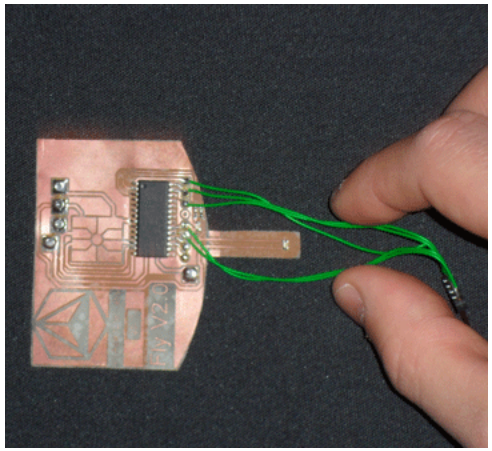
- **Do NOT turn device(s) off, but unplug only the network cable.**
- **Do NOT make any changes to device(s)!**
- **Immediately report any suspected security incident to UTSA ISO and your campus/institute CIO.**
  - May be computer, network, or paper-based activity
  - May result in
    - Loss of confidentiality
    - Compromise of integrity
    - Loss of availability
- Label approved PCI devices to help identify what not to touch in the event of a suspected security incident.

POS Terminal Fraud

- Skimming
  - Stealing payment data from the customer's credit card
  - Stealing payment data from the payment infrastructure
  - Cloning and PIN harvesting
- POS malware and man-in-the-middle attacks
  - More prevalent with EMV devices
  - Malware used to intercept random number assigned during the transaction, replacing it with a different pre-computed number
- POS fraud targets
  - PIN data
  - Unattended or unmanned terminals
  - Merchants with a high transaction volume
  - Merchants with periods of high volume sales

Identifying POS Terminal Fraud

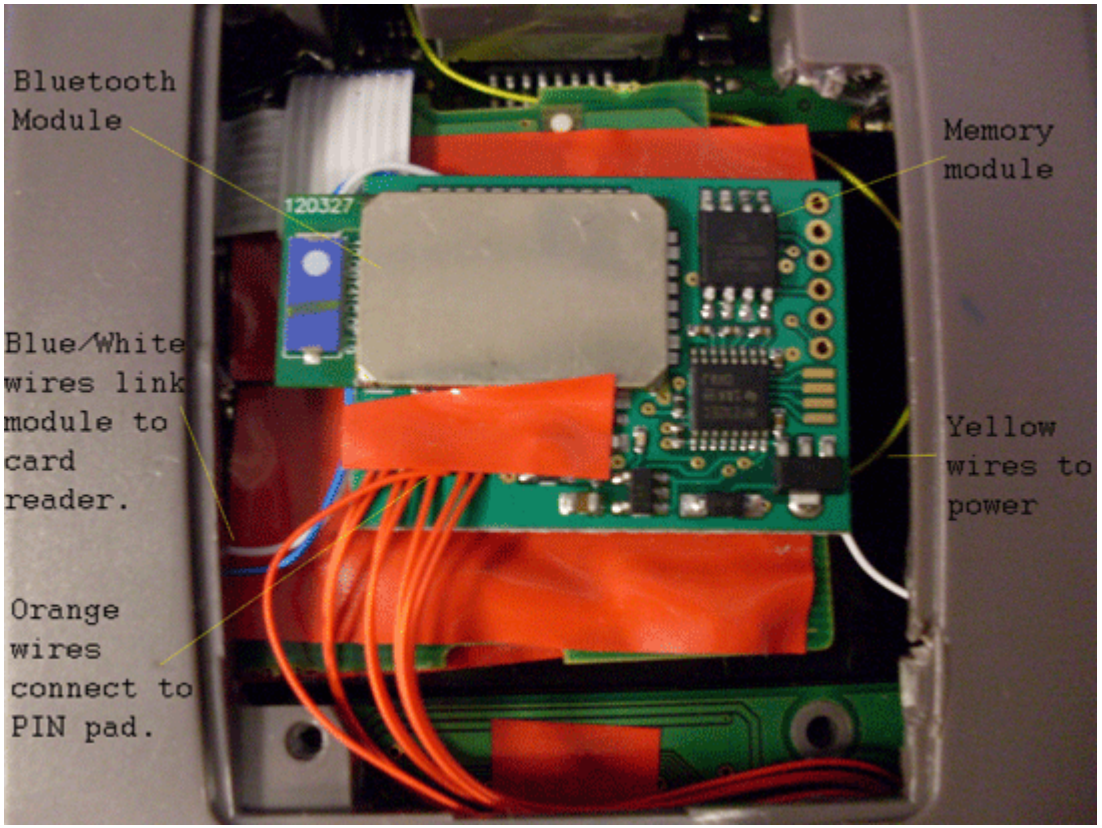
- Examples of skimming devices added to POS terminals



Skimmers can be hidden by the SIM card cover plate and by overlays, or stickers that cover the keyboard area and can hide damage due to tampering, as well as wires that allow for keyboard logging.

Identifying POS Terminal Fraud

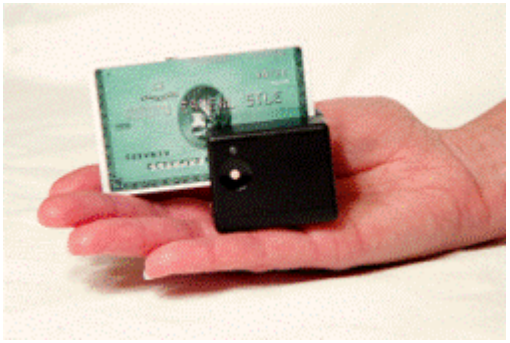
- Example of a modification to the POS circuit board



This skimmer has been soldered to the based of the existing circuit board. The blue and white wires leading from the skimmer connect the skimmer to the card reader on the POS device, while the orange wires connect directly to the PIN pad. The Bluetooth module routes the CHD to the attacker.

Identifying POS Terminal Fraud

- Examples of handheld skimmers



These small, handheld devices, often used by corrupt staff, can store a large amount of CHD and can connect to mobile devices.

Identifying POS Terminal Fraud

- Example of terminal connection change

Normal terminal connection cable

Changed cable houses additional wires to capture CHD

Identifying POS Terminal Fraud

- Remember that you are looking for signs of tampering or substitution, but you should not open the device yourself.
- Inspect terminals often to ensure there are no new stickers (could be overlays!) or that original stickers have not been removed or modified.
- Inspect terminals often to see if the serial numbers are correct.
- Inspect terminals often for broken or different colored casings, as well as loosened or missing screws.

Identifying POS Terminal Fraud

- Inspect terminal connection cables often for any signs of tampering.
- Verify the identity of anyone claiming to be a maintenance or repair person there to work on your POS device.
  - Verify who called prior to granting access to the device.
  - Do not install, replace, or return devices without authorization.
- Report suspicious behavior around POS devices.
  - Be aware of anyone handling, unplugging, or opening the device.
- If you suspect your POS terminal has been tampered with in any way, please contact the UTSA ISO immediately.

Protecting POS Devices

- Go through the Treasurer's Office for ordering POS devices.
  - The Treasurer's Office has a list of approved devices.
  - Devices ordered through the Treasurer's Office will be pre-programmed by Elavon.
- Keep terminals secured when not in use.
- If terminals are in a public location, never leave them unmanned or unattended.
- Regularly inspect the devices.
  - The more the device is used, the more often it should be inspected.
  - If the device is rarely used, always inspect before the next use.
  - Have more than one person responsible for inspection.

Protecting POS Devices

- Keep your inventory of POS devices current.
  - Use the PCI DSS Inventory Log found at http://security.tennessee.edu/pci-dss-compliance-information/.
  - This log should include each person who is approved to use the devices.
- Employees shall review this training regularly and new employees must review prior to having access to terminals.
- Allow employees role-based access to the terminals.
  - If access is not needed, access should not be authorized.
  - Access should be removed immediately upon termination of employment.

Annual Obligations

- Complete PCI Security Awareness Training
- Documentation
  - Internal policies and procedures (update as needed)
  - Policy FI0311
  - Other pertinent UT policies
- Update Inventory
  - Update list of devices
  - Update who is explicitly authorized to use devices
    - Remember to remove access immediately when an employee terminates
    - Remember to remove access if an employee no longer needs it
  - Get management authorization each time inventory is updated
  - Label devices to identify owner, contact info, and purpose

Review

- Overview of PCI DSS
- PCI DSS Compliance
- Merchants' Roles and Responsibilities
- Identifying and Reporting Data Breaches
- Identifying Fraud and Protecting the POS
- Merchants' Annual Obligations

If you have questions, comments, or concerns,

please contact
Stephen Brown at Stephen.Brown@tennessee.edu or
(865) 974-8683 or
Justin Holt at Holt@tennessee.edu
or (865) 974-2302.

Updated PCI resources are available on the PCI Compliance website:

http://security.tennessee.edu/pci-dss-compliance-information/

Training Verification

- For each merchant, every employee involved in the processing of cardholder data must complete training as part of the formal PCI Security Awareness Training.

- For your official verification of the training, you will need to answer the three short questions in this Qualtrics survey (posted 1/3/2022): https://utk.co1.qualtrics.com/jfe/form/SV_cMhgOVEDEwMW7hI
- This verification will be documented and kept on file with the UTSA ISO should you need it in the event of an audit.