POS Security Training

k14226699 fotosearch.com

k6904588 www.fotosearch.com

Table of Contents

POS Security

Dealing with the Payment Card Industry Data Security Standard (PCI DSS) is now part of the overall compliance strategy for most organizations that process, transmit or store cardholder data. PCI DSS exists to protect cardholder data processed, stored or transmitted by merchants. Payment Application Data Security Standard (PA-DSS) is a set of requirements aimed at ensuring that payment processing applications, such as those used by payment service providers and banks, are secure and do not put cardholder data at risk.

PIN Transaction Security (PTS), however, is concerned with the physical and logical security of the point-of-sale devices or terminals, whether they be attended, i.e. manned by merchants, or unattended, i.e. parking payment automated machines.

Merchants have an obligation to ensure their respective payment systems and infrastructures are secure. Merchants are the first line of defense for POS fraud and are involved in the execution of the vast majority of controls suggested or required by PCI SSC. Merchants can achieve appropriate security and trust levels at the point of sale by considering all the factors that can influence overall security in their terminal environment and taking the necessary countermeasures detailed in this document.

Objectives

- To comply with PCI Requirements 9.9, 9.9.3, 12.4, 12.6 and 12.10.1
- To communicate training and awareness of security responsibilities to all persons with direct contact to POS devices

Inspection Frequency Information

PCI version 3.0 requires merchant to maintain a list of their POS devices, conduct regular inspection, have an understanding when a device was tampered or compromised and aware on how to respond in the event of a breach or compromise. The PCI Working Committee approved to implement the quarterly submission of inspection log and the attachment of tamper proof security seal on all POS devices. It is recommended to do the inspection on a monthly basis.

Schedule of Submission

Quarter	Month
1	July
2	October
3	January
4	April

It is the responsibility of the merchant to inspect the POS device daily before using to ensure that the security seal is intact.

POS Inspection log should be submitted to the PCI Compliance Officer quarterly, in compliance with PCI Requirements 9.9.1 and 9.9.2 (version 3.0).

DO NOT USE the POS device if there is evidence of tampering, e.g. broken seal, unscrewed parts, different cable, etc.

Inspection Process

Conduct daily checks

Routine inspections of your premises will help you uncover card-reading devices and other illegal equipment before fraudsters get a chance to use them

Take care with your terminal

Your PIN pad is just as valuable as cash to criminals, so treat it just as carefully.

Know your staff

Fraudsters can operate as easily within your business as outside, so it's important to practice due diligence when hiring and supervising employees.

Pin Pad Serial Number Inspection

✓ Check the serial number of both the terminal and PIN pad to ensure both devices haven't been switched for a device fraudsters use to "skim" or collect magnetic strip data and PINs.

Security Seal Inspection

✓ Check the PIN pad for signs of tampering - broken or replaced parts or security seal.

Evidence of PIN Pad Tampering Inspection

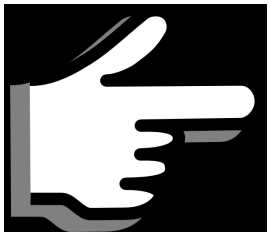
- Terminal stickers providing details of the product and serial number were broken
  - ✓ Note the serial number on the back of the terminal and check this against the electronic serial number
  - ✓ Run your finger along the label to check that it is not hiding a compromise
- UBC security seal was broken
  - ✓ Check if the seal has been cut or removed or replaced or substituted with a counterfeit seal
- Screw holes or seams indicated that the device has been opened
  - ✓ Check the label position, color and materials used
  - ✓ Look for any signs that the label may have been removed or tampered with
- Skimming device inserted in a terminal (hidden by the SIM card cover plate)
- Handheld skimmers used by corrupt staff
  - ✓ Check the SIM card cover plate for any attached devices
- Unfamiliar electronic equipment connected to the terminal or cash register or network connections
  - ✓ Examine any connection of strange or unusual equipment
- Unannounced service visits from TD or Moneris
  - ✓ Require all repair technicians who visit your location to sign in, verify their identity with photo ID, and remain accompanied by staff during any work on PIN pads

Evidence of Cable Substitution Inspection

- Key loggers attached to the cable
  - ✓ Examine the cable attached to the device for any small equipment that can look like part of the normal cabling
- Changes to terminal connections
  - ✓ Examine any changes to the cable used to connect the terminal to the base unit or any additional wires not part of the cabling
- Devices connected into the telephone exchange
  - ✓ Inspect telephone boxes for devices that record transmissions like voice recorders or MP3 players

Physical Security Inspection

- ✓ Securely mount PIN pads securely to the counter or keep out of reach from unauthorized users
- ✓ Have visual inspection performed on every device to look for potential signs of tampering - **DO NOT USE** if the seal is broken
- ✓ Ensure security cameras have a clear line of sight to the PIN pad terminals to aid investigators in the event of a security compromise
- ✓ Store spare devices under lock and key to prevent unauthorized removal
- ✓ Require all visiting repair technicians to sign in with their name and company information
- ✓ Change the device's default admin password
- ✓ Request for POS device must be centrally approved and should come only from UBC's authorized provider
- ✓ Contact ITSC (to report incident), campus security and law enforcement if evidence of tampering or device substitution is found



Have an incident response communiucations plan in place. Most effective incident response plans include personnel and processes with the lists and channels needed to execute all communications that might be needed.

Security guidelines and best practices

- Inspect your POS equipment regularly - If anything looks unfamiliar, appears altered, or is missing, notify your supervisor immediately.
- Ensure you provide customers with enough room to comfortably shield the PIN pad when entering their number.
- Make sure that any security cameras on your premises don't capture the PIN that customers are entering.
- Allow the customer to hold the PIN pad until the transaction is complete, and never enter a PIN for a customer.
- Check ceilings, walls or shelves near PIN pads on your premises for holes that could conceal a small camera.
- When not in use, place the PIN pad under the counter or out of customers' reach (but do not unplug).
- Institute a procedure that requires all visiting repair technicians to sign in with their name and company information and to track the serial numbers of any devices that are installed, removed and/or replaced.

Appendix – Reference Images

Appendix – Reference Resources

- Point of Sale – Security Recommendations
- Skimming Prevention – Best Practices for Merchants
- TD Fraud Awareness
- Moneris Merchant Operating Manual
- Interac Debit Card Fraud Prevention
- VISA PIN Security – Tools and Best Practices for Merchants

Appendix – POS/PIN Pad Inspection Log

POS / PinPad Inspection											
Date	Employee Name / Initials	Merchant Account #	Model #	Terminal Serial Number/ UBC Seal#	Terminal Serial Number Confirmed (Yes / No)	PIN Pad Serial Number/ UBC Seal#	PIN Pad Serial Number Confirmed (Yes / No)	Security Seal Intact (Yes / No)	Evidence Of PIN Pad Tampering (Yes/No) (see Images)	Evidence of Cable Substitution (Yes / No) (see images)	Physical Security Intact (Yes / No)
10-Jul-14	Raul Ramos	xxxxxxxx	TD Freedom IV	Taxxxxxx/XXXX	Yes	TVxxxxxx/YYYYY	Yes	Yes	No	No	Yes
August											
September											
October											
November											
December											
January											
February											
March											
April											
May											
June											