

PIN Pad Security Best Practices



Introduction

The payment industry and card associations adopted PED and PCI PED requirements because of concerns that sophisticated criminal organizations may have the resources to tamper with PED terminals to install a bug and collect private card data. In Pre PED devices, security features were left to each vendor to determine. The more recently adopted Visa PED and PCI PED requirements provide standardized security features that make tampering progressively more difficult.

We are seeing an increase in criminal organizations targeting the less secure pre PED terminals by installing bugs to collect private credit card and debit information. In these cases, the criminal organizations are inserting a bug into an in-place device or obtaining the same terminal model that a retailer uses, installing a bug, and then substituting the tampered device for the retailer's terminals. They then either come back to retrieve these terminals to obtain the stolen information, or in some cases, the tampered terminals send the information to another computer via wireless communications.

Due to repeated targeting of pre PED PIN pads and payment terminals, VeriFone has developed the following PIN Pad Security Best Practices. These best practices first enable a retailer to determine if any existing terminals have been tampered with, and second make tampering much more difficult by implementing a comprehensive set of security controls to prevent tampering and more quickly become aware if tampering has occurred.

This document details the PIN Pad Security Best Practices from a sound security perspective to minimize fraud through education, routine inspection, vendor management, and prompt action. Each of the Best Practices are organized into the following categories:

1. Administrative Activities – This category covers items that include employee education on data security theft, and common prevention activities.
2. Physical Activities – This category includes items involving physical inspection of payment system components.
3. Technical Activities – This category addressed data encryption and serial number validation with the POS.

To encourage reading of these best practices they have been condensed and categorized into a one page Quick Reference Guide

VeriFone recommends all retailers implement the following PIN Pad Security Best Practices immediately. If a retailer does not enact a complete PIN pad security program, including PIN Pad Security Best Practices, then they will remain vulnerable to this kind of tampering.

PIN Pad Security Best Practices Quick Reference Guide

| | Prevention | Detection | Correction |
|----------------------------------|---|--|---|
| Administrative Activities | Educate store employees about the techniques criminals use | | |
| | Update new employee training curriculum to include security awareness | | |
| | Instruct all employees to be vigilant in looking for suspicious activity around pumps | | |
| | Change default PIN Pad passwords. | | |
| | Monitor PIN Pad payment problems | | |
| | Check the accreditations / references of any service technicians. Require they show ID and sign a service log | | |
| | Use and retain accurate shift schedules so that a staff audit trail is available | | |
| | | Periodically audit the service log | |
| | | | |
| | Check repair technician verification and service log | | |
| | Store PIN Pad and payment terminals in a secure location | | |
| | Track terminal assets as they move in and out of inventory | | |
| | Only purchase payment terminals from authorized sources | | |
| | Use only authorized repair centers | | |
| | Securely dispose of retired terminal inventory | | |
| | Develop a response plan in advance in case a breach occurs | | |
| Physical Activities | Mount PIN Pads securely to counter | | |
| | Visually inspect terminals weekly | | |
| | | Focus security cameras on terminals; maintain CCTV data logs for use later | |
| | | | Call Law Enforcement if device tampering is found |
| Technical Activities | Encrypt data from the PIN Pad | | |
| | Validate all serial numbers manually with the serial number printed on the bottom of the terminal | | |
| | Validate all terminal serial numbers electronically with the POS | | |
| | Authenticate all payment applications | | |

Administrative Activities

1. Educate your store employees and managers about the techniques criminals use to breach PIN Pads and payment terminals.

Data thieves have sophisticated equipment that can be installed in minutes. Store employees should be educated as to the type of equipment data thieves install, where they typically install it, and what information they can gain once it is installed.

2. Update new employee training curriculum to include the techniques criminals use to breach PIN Pads and payment terminals.

New employees should be trained to be on the lookout for suspicious activity around the PIN Pad or payment terminal, and who to call should such activity be cause for concern.

3. Change Default PIN Pad Password

Make sure the password for device access is not the original default password. If it is, have it changed, as default passwords become widely known. Contact your account executive if you need help changing this password.

4. Monitor PIN Pad Payment Problems

Develop a process to monitor devices that consistently do not work properly such as high mag-stripe read failures or debit card declines. These can be indicators of tampered terminals. Contact the security officer at the terminal manufacturer to determine the next steps.

5. Check the accreditations / references of any service technicians. Require they show a photo ID and sign a service log

Social engineering is sometimes employed to commit fraud; a fraudster acts as a service technician or consultant to allow them to gain unauthorized access. All service technicians should be required to show a photo ID and sign a service log. The details of the visit should be communicated in advance to the manager or cashier by management.

6. Use and retain accurate shift schedules so that a staff audit trail is available

Schedules of "what staff worked when" should be maintained to help with any investigations or enquiries that may arise at a future date. This will also act as a deterrent to staff to commit fraud as they are accountable for their actions.

7. Periodically audit the service log

Establish and maintain a service log that records the who/what/where/when/why of a technician visit should be periodically audited by management to ensure that all servicing was approved.

8. Check Repair Technician Verification and Log Service Activities

Implement a procedure to require all repair technicians who visit your stores sign in, verify their identity with photo identification, and remain accompanied by store personnel during any work on PIN pads.

9. Store PIN Pad and Payment Terminals in a Secure Location

Store all spare devices under lock and key to prevent unauthorized removal. Incorporate a procedure to validate the devices inventory at every shift and have not disappeared.

10. Track Terminal Assets as they move in and out of Inventory

Institute a procedure to track every time a terminal is replaced within the store, whether from the in-store inventory, by a repair technician, or units shipped into the store

11. Purchase from Authorized Sources

Only obtain PIN pads from a manufacturer or manufacturer's authorized partner. Unauthorized resellers, such as may be found online at sites such as eBay, may potentially sell devices that are already compromised, whether intentionally or unwittingly.

12. Use Authorized Repair Centers

For similar reasons, have your PIN pads repaired at the manufacturer or an authorized manufacturer's repair center which has completed a TG3 Key Injection audit.

13. Securely Dispose of Retired Terminal Inventory

In order to properly dispose of retired terminal inventory, only use firms that destroy the encryption keys during the retirement and recycling process. Select environmentally friendly destruction facilities that recycle all metal and plastic components, and follow proper hazardous material destruction procedures for PCB components. For PCI compliance verification, consider firms that issue an inventory disposal report that lists all terminals being retired by their serial number.

14. Develop a Response Plan in Advance!

Develop methods and procedures on how to handle subsequent activities should a breach occur. Determine who in your company will be the go-to person or coordinator of all breach-related activity. How do you respond? Who do you need to call first? Can you respond internally or should a third party be involved? Who is the third party? How do you manage external communications? What internal systems are involved in the breach? Do you keep accurate records of all system change activities for all of your sites?

Physical Activities

1. Mount PIN Pads Securely to Counter

Review the installation of your PIN pads. They should be mounted on the counter; unplugging cables should require more than turning the unit over; and you may want to consider installing locking stands to prevent unauthorized removal.

2. Weekly Visual Terminal Inspections -

Immediately have a visual inspection performed on every device to look for potential signs of tampering. These include anything that does not look normal such as lack of tamper seals, damaged or altered tamper seals, mismatched keys, missing screws, incorrect keyboard overlays, external wires, holes in the terminal or anything else unusual. Look for hidden cameras in the ceiling and inspect non-secured wiring. If anything out of the ordinary is noticed, stop using the device, disconnect it from the pos terminal or network, but do not power it down. Contact the security officer at the terminal manufacturer to determine the next steps. Continue to perform visual inspections weekly.

3. Focus Security Camera's on PIN Pads

Ensure security cameras have a clear line of sight to the PIN Pad terminals to aid investigators in the event of a security compromise. Images of data thieves and the methods they are using is invaluable information. Front orientation cameras provide the best evidence without interfering with customer's actual PIN entry on the payment devices.

4. Contact Law Enforcement if Evidence of Tampering or Device Substitution is Found

Law enforcement needs to be involved if there is any suspicion of data theft crime. They will engage experts who need to respond quickly in order to apprehend the criminals.

Technical Activities

1. Encrypt Data from the PIN Pad

As Terminal Physical Security Has Increased, Criminals have turned to tapping the connection between the PIN Pad and the POS Terminal, or From the POS Terminal to the Communications Equipment. All sensitive customer data should be encrypted before it leaves the PIN Pad

2. Serial Number Validation

If your terminal contains an electronic serial number, have the electronic serial number compared to the serial number printed on the bottom of the terminal. If these do not match stop using the device, disconnect it from the POS terminal or network, but do not power it down. Contact the security officer at the terminal manufacturer to determine the next steps.

3. Electronic Serial Number Validation

If the PIN Pad supports electronic serial numbers, implement a scheme to validate the Pin Pad serial number every time the POS. starts up to insure the device has not been replaced, and if it has, automatically send an alert. If the device supports Ethernet connectivity, consider implementing a device management solution to track all in service devices.

4. Authenticate Applications

To insure rogue applications are not installed on the PIN Pad and access to ports are controlled all applications should utilize the vendor's method of authentication. Insure the default certificates are changed prior to deployment.

Reference Documents

1. POS/POI Terminal Security Best practices to application developers, system integrators, and end users, MasterCard, February 2006, Draft V02
2. Visa Fraud Prevention for merchants (<http://merchants.visa.com/prevention/main.jsp>)
3. Payment Card Industry (PCI) Data Security Standard (<https://www.pcisecuritystandards.org>)
4. Fuel Dispenser Payment Security Best Practices V1, VeriFone Inc, October 2008
5. VeriFone's Retail Payment Security website, www.secureretailpayments.com.