Date of Last Revision: September 2024
Responsible Department: Information Technology

How-To Guide for Device Inspections

1. PERIODIC DEVICE INSPECTIONS

According to PCI DSS, physical inspections of terminals must be conducted periodically.

https://www.pcisecuritystandards.org/documents/Skimming_Prevention_BP_for_Merchants_Sept2014.pdf?agreement=true&time=1542344769638

GVSU requires inspection as part of daily procedures. A quick review of each terminal will take just a moment and will help a potential security incident.

Employees need to maintain a log of these security checks for each device. GVSU has made this available as a Microsoft Office form available at: https://forms.office.com/r/N3hW0W4tBE.

2. CHECKING FOR SUBSTITUTION

Staff must verify on a regular basis that the device inventory list is reconciled against the devices in use, as criminals may try to replace devices with tampered units. During the inspection, make sure to cross check identification numbers with the form. Most devices will have a sticker attached to the bottom, which provides details of the product and generally include a serial number (see image below).

The majority of terminals will also have a method of displaying the serial number electronically. When powered on, the device serial number reported should match the serial number on the device itself. Verify that the serial number (or module number, part number, etc.) on the form match with the devices currently in use.

It is also important that staff verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. Require that visitors check in upon arrival and train all onsite personnel to verify the visitor's identity and purpose of visit. This is an important step as multiple organizations have suffered breaches after criminals, appearing to be authorized maintenance crews, were provided physical access to devices. Criminals have also been successful by simply sending fraudulent devices to a location with instructions to install and deploy them. Make sure you know the policy and procedures for issuing and installing payment card devices so only approved devices are deployed.

3. CHECKING FOR TAMPERING

Credit card skimming devices are designed to blend in seamlessly with the machine it's placed on. Unless you are specifically looking for a skimming device, you may not notice anything out of the ordinary.

Look over the device thoroughly and check for any unusual gaps or signs of tampering. Manufacturers will often use tamper evident stickers, so any attempts to open the outer casing of devices is apparent. If a criminal has attempted to compromise a terminal, they may remove these stickers or replace them with their own printed versions. This is an example ID Tech SRED Key device with a tamper sticker.

Staff should also be aware of the use of overlays. An overlay, often created on a 3D printer, is a small piece of plastic that fits closely to the device and attempts to maintain the original look or hide evidence of tampering. The greatest risk posed by these overlays is their inclusion of an additional payment card reader that grabs a copy of the cardholder data for later use in fraudulent transactions. In the example image, the terminal on the left has an overlay over the top of the device. Any payment cards swiped through this terminal would have their cardholder data stolen and, until the overlay was detected, no one would be the wiser.

Criminals can also insert electronic equipment into the terminal to capture cardholder data. This equipment, called a shimmer, can be very sophisticated, small, and difficult to identify. Often it is hidden inside the device so neither the merchant nor the cardholder can tell that the terminal has been compromised from the outside. When you insert your card into the chip slot, the reader reads the data from the chip on your card. There may be a difference in how the card now inserts, as you can see from the image below. It is also possible to identify if a shimming device has been inserted by weighing the device and checking for any difference.

Staff should include the following in their tamper checking procedures:

- ✓ Is the device in its designated location?
- ✓ Is the color and condition of the device as expected, with no additional marks or scratches?
- ✓ Are parts of the card reader loose? Or does anything move or wiggle when pulled on?
- ✓ Are there any loose or missing screws?
- ✓ Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
- ✓ Is the number of connections to the device as expected, with the same type and color of cables?
- ✓ Is the pin pad thicker than normal?
- ✓ Are there any unauthorized electronic devices (phones, iPods, etc.) near the device?
- ✓ Inspect the ceiling area above the POS device for cameras.

4. INCIDENT RESPONSE

As part of your Incident Response Plan, verify you know how and where to report any suspected tampering or substitution. If a skimming device is found, you should immediately stop using the payment card terminal and disconnect it from the network. Take pictures and document all evidence.

If a skimming device is detected, the smaller the window between discovery and last clean inspection, the smaller the potential impact for compromised records.

With the advancement of 3D printing and criminals becoming more advanced in their methods, skimming is becoming more of an issue. There are proven criminal cases of skimmers being installed in as little as 3 seconds. Surveillance of payment systems and regular inspections will help keep your customers safe and help you to be more alert consumers when using payment cards.