Kiosk Physical Security Audit

Kiosk Physical Security

This document will show you how to conduct a physical security inspection of your kiosks. Knowing that your kiosks are physically secure is important to ensure the safety of consumers and their data. Operators are encouraged to do a physical inspection of the kiosk each time they restock the store.

Checking for Credit Card Skimmers

- Inspect the card reader. Does it look natural? Does it appear that it has been altered?
- Pull on the card slot. Be sure that no foreign device has been installed.

365 card readers are displayed below. If the card reader is different than the ones listed below, call 365 Support and we can help investigate the type of card reader installed.

OTI DUO Card Reader

IDTech Card Reader

Most card skimmers are devices that are attached to the external components of a card reader. The best defense against such devices is a close review of the card reader as explained above. Below is an example of a device that attaches to the outside of a card reader.

Kiosk Physical Security Audit

With the advancement of technology, new card skimmers have been developed that are inserted inside card readers. These devices are slightly harder to detect, but with proper review of the card reader they can be spotted. When inspecting your kiosk for such devices thoroughly inspect the outside of the card reader and look inside the card slot as well. Below is an image of a recovered internal card skimmer.

Inspect the locks on your kiosk

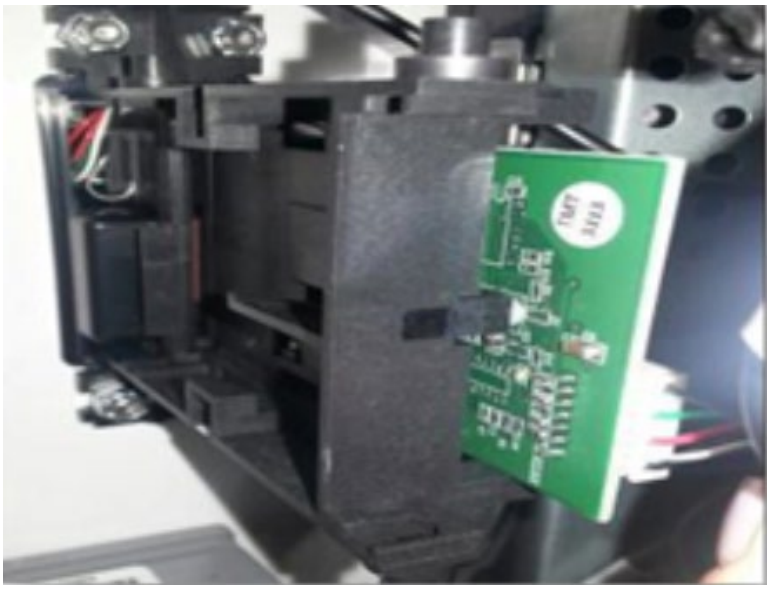
- Is the kiosk currently locked?
- Inspect all locks located on the kiosk. Do they look like they have been forced open? This would result in obvious damage to the locking mechanism.

We use several different types of locks on our kiosks. Our Gen 2 kiosk uses two different types:

- T-handle Lock
- Tubular Cam Lock

Inspect the Back Side of the Card Reader

- Are there any foreign objects attached to the back of the card reader?
- Pull on the back of the reader carefully to ensure everything is secure.



Back side of IDTech Card Reader

Look for Key Loggers or Devices Plugged into the Card Reader

- Inspect the end of the USB connecter from the card reader.
- Are there any devices plugged in between the card reader and the computer?

Card Reader Plugged In

Card Reader Unplugged

Key Loggers

Below is an image of a common key logger. It is very unlikely that you will ever see one of these, but it is good to know what to look for. These devices are installed between the card reader and the computer. If you see one of these devices take a photo and send to 365 Support (support@365smartshop.com).

Reviewing DVR Footage

When an incident is reported, it is vital to review video footage of the date and time the incident was reported or suspected to have occurred by operator or customer. If a DVR is not in place, the operator of the kiosk should contact the local company and request that this footage be reviewed, and the same process followed.

This is a manual process that the operator is responsible for since 365 Retail Markets does not have access into these camera systems. Physical evidence of device tampering is crucial to completing our Incident Response process as it can display criminal activity, device tampering, system malfunctions, power outages or application errors.