Risk Control Bulletin

Seven Tips to a Point of Sale Security Inspection

We can show you more.®

RISK CONTROL

Implementing a daily inspection of all point of sale (POS) credit card readers for evidence of tampering may identify a security breach sooner rather than later. Below, we've outlined seven key tactics to include as part of the inspection process.

1. Train Employees to be Aware

Teach employees how to spot indications of tampering. Covert installations of card skimmers such as additional hardware near the legitimate card reader or miniature cameras to record pin numbers are things to lookout for.

2. Take Inventory

Take inventory of all devices that collect data at all locations. Make sure to include devices not only at point of sale areas but self-service areas as well.

3. Share the Responsibility

Rotate the responsibility for the inspection to different employees – and assign each employee a unique user account – as often as practical. This will limit the possibility of an insider installing such hardware and avoiding detection. Make sure the employee conducting the inspection acknowledges the condition of each device at time of inspection.

4. Log Results

Require employees to log their entries upon completion of each inspection. Things such as the date and time of inspection, completed & signed inspection checklist, notes on inspection results if tampering or suspicious devices are detected are all important to track.

5. Plan Ahead

Have a process identified in case a device appears to have been tampered with. These devices should be removed and safely stored for investigative purposes and referral to law enforcement.

6. Engage Management

Include management as part of your process to ensure that in case of a breach, employees know who should be notified so that they can notify proper law enforcement so investigation can begin.

7. Limit Internet Connectivity

Do not allow access to websites through your POS network. POS networks can be segmented to limit access to the internet, while still allowing access to only approved Anti-Virus updates and POS security logs. All other internet activity should not be allowed.