Digital Payments
for a Trusted World

WORLDLINE

Skimming-Prävention am Terminal im Innen- und Aussenbereich

Verhindern Sie Betrugsfälle, sogenannte Skimming[1]-Fälle, an Ihren Verkaufspunkten sowohl im Innen- wie auch im Aussenbereich. Erkennen Sie Manipulationen am Terminal frühestmöglich und leiten Sie die richtigen Schritte ein. Sie als Händler tragen zusammen mit Ihren Mitarbeiterinnen und Mitarbeitern entscheidend dazu bei, finanziellen Schaden zu verhindern oder zu minimieren.

VORBEREITUNG: TERMINAL/AUTOMAT IM ORIGINALZUSTAND FOTOGRAFIEREN

Erstellen Sie von jedem sich in Betrieb befindenden Terminal/Terminaltyp zwei Fotos:

- vom Karteneinzug
- vom Tastaturblock, über welchen der Geheimcode (PIN) eingegeben werden muss

Die Fotos dienen als Vergleichsmöglichkeit für die empfohlenen täglichen Kontrollen. Entdecken Sie dadurch Vorrichtungen, die für Skimming-Zwecke angebracht worden sind.

TIPPS ZUR TÄGLICHEN KONTROLLE

Überprüfen Sie am Morgen, am Mittag und/oder am Abend jeweils nach dem Eintreffen bzw. beim Verlassen der Arbeit die folgenden Module auf Manipulation.

Verwenden Sie dazu die Original-Fotos und vergleichen Sie diese mit:

- dem Tastaturblock und dem Karteneinzug (Slot) des Terminals
- allen Bereichen am und rund um die Verkaufspunkte, welche mit einer Miniatur-Kamera mit Blickfeld auf die Tastatur versehen werden könnten.

Auch wenn vor allem Automaten im Aussenbereich gefährdet sind, empfehlen wir Ihnen, ebenfalls die Terminals im Innenbereich zu kontrollieren.

BEI VERDACHT AUF MANIPULATION GEHEN SIE WIE FOLGT VOR:

1. Lassen Sie keine Zahlungen beim betroffenen Terminal mehr zu.
2. Entfernen Sie **keine** Skimming-Vorrichtungen (z.B. Aufsätze bei Kartenslots, Miniatur-Kameras etc.) vom betroffenen Terminal/Automaten.
3. Wenn ein Terminal/Automat im Aussenbereich betroffen ist: Entfernen Sie sich davon, denn die Täterschaft könnte noch in Sichtweite sein.
4. Informieren Sie sofort den nächsten Polizeiposten.
5. Melden Sie uns den Vorfall schnellstmöglich unter Angabe der Terminal-ID, des Terminal-Standorts, Zeitpunkts der Feststellung sowie der letzten Kontrolle an (EU: Fraud_eu@worldline.com, CH: fraud@worldline.com).

[1] Skimming = Engl. «Abschöpfen». Beim Skimming werden Terminals so präpariert, dass die Täterschaft in den Besitz von Magnetstreifendaten von Karten und den entsprechenden PINs gelangt. Mit dem Anbringen eines vor dem Kartenleser montierten Aufsatzes mit Magnetspur-Lesekopf und mit einer Miniatur-Kamera oder Tastaturattrappe werden die entsprechenden Daten erfasst.

Ihren lokalen Ansprechpartner finden Sie unter: worldline.com/merchant-services/contacts

110.0011.01 INT_DE/12.2021