Digital Payments
for a Trusted World

WORLDLINE

Prevenzione dello skimming ai terminali di pagamento interni ed esterni

Prevenite efficacemente le frodi, i cosiddetti casi di skimming[1], ai vostri punti vendita interni ed esterni. Riconoscete tempestivamente eventuali manomissioni del terminale e avviate le necessarie contromisure. In qualità di esercenti, voi e i vostri collaboratori potete contribuire in modo determinante ad evitare o minimizzare i possibili danni finanziari connessi a tali frodi.

PREPARAZIONE: FOTOGRAFATE IL TERMINALE DI PAGAMENTO/DISTRIBUTORE AUTOMATICO NEL SUO STATO ORIGINALE

Scattate due foto di ogni tipo di terminale di pagamento in esercizio:

- una foto della fessura d'inserimento della carta
- una foto del tastierino per l'immissione del codice segreto (PIN)

Le foto servono quale riferimento per i controlli giornalieri raccomandati. Riconoscerete così per tempo la presenza di dispositivi applicati a scopo di skimming.

CONSIGLI PER IL CONTROLLO GIORNALIERO

Verificate la mattina, all'ora di pranzo e/oppure la sera, all'arrivo e al momento di lasciare il lavoro, la presenza di eventuali segni di manomissione dei moduli indicati qui sotto.

Utilizzando le foto originali, confrontatele con:

- il blocco del tastierino e la fessura d'inserimento della carta (slot) del terminale di pagamento
- tutte le aree presso il punto vendita e circostanti a esso nelle quali potrebbe essere stata installata una mini-camera in grado di inquadrare il tastierino

Sebbene siano prevalentemente minacciati i distributori automatici installati all'esterno, raccomandiamo di controllare anche i terminali di pagamento presenti nelle aree interne.

IN CASO DI SOSPETTA MANOMISSIONE DEI DISPOSITIVI, PROCEDETE COME SEGUE:

1. Impedite che vengano effettuati ulteriori pagamenti al terminale in questione.
2. **Non** rimuovete dal terminale/dal distributore automatico lo strumento impiegato per lo skimming (dispositivo applicato alla fessura d'inserimento della carta, mini-camera, ecc.).
3. Se il terminale di pagamento/distributore automatico si trova all'esterno, allontanatevi da esso: gli autori della frode potrebbero trovarsi ancora nelle vicina.
4. Informate immediatamente il posto di Polizia più vicino.
5. Ci segnali per favore il prima possibile quanto è accaduto, indicando l'ID del terminale, l'ubicazione del terminale, il momento del rilevamento e l'ultimo controllo (UE: Fraud_eu@worldline.com, CH: fraud@worldline.com).

[1] Skimming: dall'inglese «schiumare». Nello skimming, i terminali di pagamento vengono manomessi in modo tale da consentire agli autori della frode di entrare in possesso dei dati registrati sulla banda magnetica della carta e del relativo PIN. I dati vengono raccolti mediante un dispositivo dotato di testina di lettura della banda magnetica, applicato davanti al lettore, ed una mini-camera o una finta tastiera.

L'interlocutore locale è indicato su: worldline.com/merchant-services/contacts

110.0011.04 INT_IT/12.2021