Un Pos mobile per rubare soldi da carte e telefoni tenuti in tasca: il «borseggio 2.0» è una realtà? E come proteggersi?

Sono tornati i video virali in cui i ladri si aggirano tra la folla con un Pos mobile e sfruttano i pagamenti senza contatto per prelevare piccole somme dai passanti ignari (distratti da un complice): ma è possibile o è solo una leggenda metropolitana? Il caso di una donna arrestata a Sorrento (Fonte: https://www.corriere.it/ 1° agosto 2025)

Da Milano a Roma fino a Napoli, c'è una psicosi legata a **fantomatici furti avvenuti attraverso l'impiego di Pos portatili**. In parte dovuta al riemergere sui social di (vecchi) video virali, falsamente proposti come girati in Italia ma provenienti da paesi ben diversi (e con il sospetto che siano filmati realizzati ad arte, con attori e attrici nelle parti dei sedicenti borseggiatori 2.0). In parte però perché è di pochi giorni fa l'arresto a Sorrento di una donna di 36 anni: fermata dalle forze dell'ordine per furto di una banconota da 100 euro, le è stato trovato **un Pos portatile nella borsa**. Tra i reati contestati, spicca un furto ai danni di una turista a Roma, in cui venne sottratto un importo di circa 9.000 euro con un pagamento su un dispositivo come quello sequestrato. In questo caso si tratterebbe di una vera e propria truffa, anche piuttosto grossa visto l'importo.
Ma il caso ha rilanciato una questione che anni fa era già stata archiviata come una sostanziale bufala: **è possibile rubare soldi dalle carte (di credito o debito) o dagli smartphone, avvicinando un Pos portatile** alle tasche dei passanti e sfruttando la capacità dei pagamenti «contactless», senza Pin?

Come funzionano i pagamenti

Per rispondere alla domanda andiamo con ordine, partendo dai **Pos mobili**. Sono dispositivi portatili, in genere utilizzati da professionisti o hobbisti per ricevere denaro attraverso carte di credito, o pagamenti digitali come smartphone, dispositivi indossabili e così via.

I pagamenti elettronici (o «contactless») avvengono tramite il contatto tra il Pos e lo smartphone o tra il Pos e la carta. In entrambi i casi, **non è affatto facile sottrarre soldi da persone ignare**. Per lo smartphone, in particolare, è quasi impossibile: viene richiesta l'autenticazione prima che avvenga la transazione, anche per importi di entità ridotta, attraverso un Pin/password o un'autenticazione biometrica (volto o impronta). Alla base della tecnologia di pagamento contactless c'è **l'Nfc** (Near Field Communication).

Discorso diverso per l'acquisto tramite carta di credito, che **richiede l'inserimento del Pin** soltanto sui pagamenti al di sopra di 50 euro.

Nel caso del telefono, i dispositivi comunicano in modo che lo smartphone riferisca al dispositivo Pos un token (cioè, molto in breve, un codice) che **assicura l'anonimato della carta di pagamento dell'utente**. Una volta autorizzato l'acquisto, la banca è in grado di associare il token all'utente e approvare o rifiutare la transazione.

A differenza dello smartphone, invece, **le carte contactless dispongono di chip Emv** (Europay, Mastercard, Visa) **che genera codici di sicurezza dinamici ad ogni transazione**. Anche in questo caso interviene la tecnologia Nfc e **viene generato un token univoco**. Il circuito bancario del venditore così «interroga» quello dell'acquirente **per verificare che vi siano fondi disponibili.** Nel giro di pochi secondi potrà infine accettare o rifiutare il pagamento.

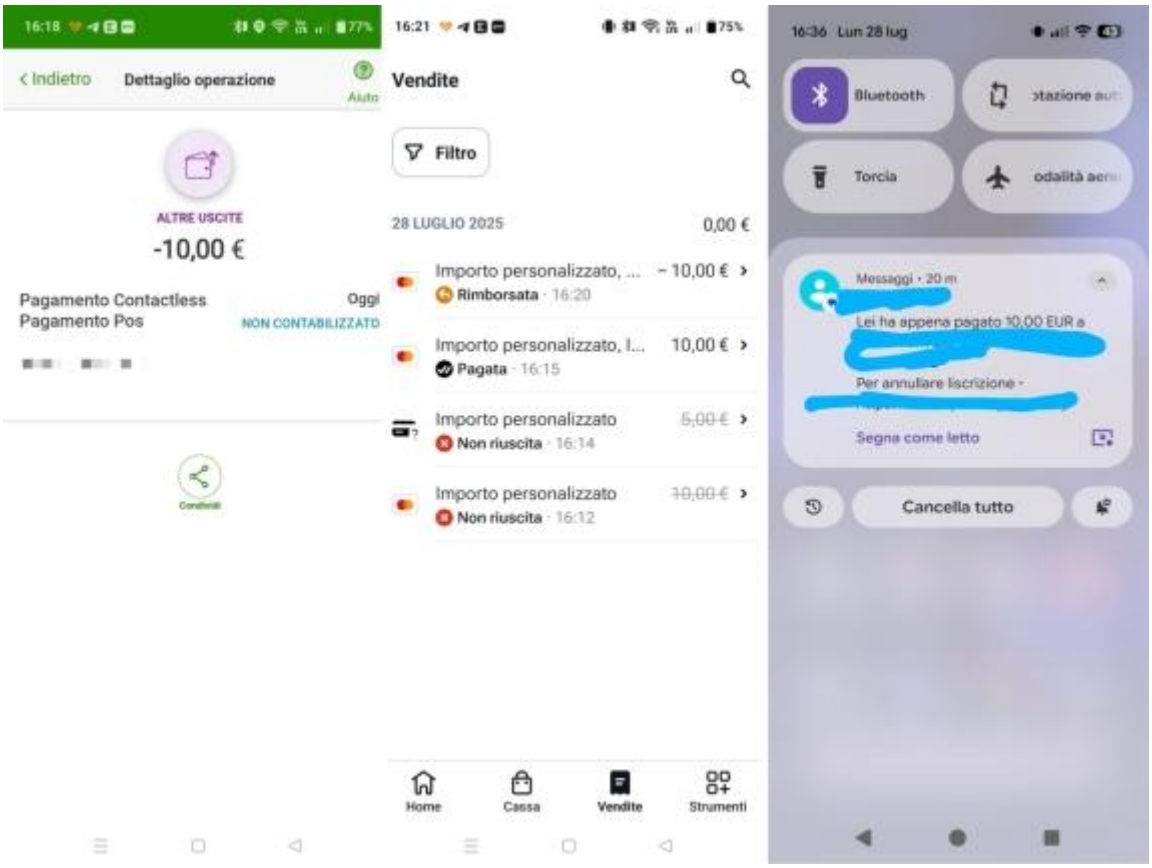
La sicurezza e i furti

Alla base di tutto, insomma, ci sono due banche che «dialogano» fra di loro in frazioni di secondo e nel caso di una truffa potrebbe essere facile risalire al malintenzionato. **Ma quando si verificano furti come quello attribuito alla donna arrestata a Sorrento**? Una possibilità è che la donna abbia **sottratto in maniera «tradizionale» delle carte di credito per poi farle appoggiarle sul proprio Pos**, ma prelevando solo cifre contenute, in modo che non fosse necessario inserire ogni volta il Pin della carta e che le transazioni passassero sotto traccia. Ad ogni modo, il Pos deve essere associato a un conto a lei riconducibile e questo non rende le cose facili agli aspiranti borseggiatori 2.0.

Come accorgersi di essere stati derubati

Per comprendere come smascherare questa potenziale forma di «furto 2.0» abbiamo usato un **Pos mobile** e lo abbiamo configurato con un conto a nostro nome. Inserendo nel dispositivo l'acquisto di un articolo da 10 euro, abbiamo «strusciato» il Pos accanto al nostro portafoglio in cui è conservata la nostra carta di credito. **Su tre tentativi, solo uno è andato a buon fine**.

È importante sottolineare che per poter utilizzare il servizio come venditore è necessario **inserire il codice fiscale e una foto fronte e retro della nostra carta di identità, oltre ad un breve video di registrazione del nostro volto**. Un processo fondamentale perché il «conto venditore» sia attivato. E, al tempo stesso, è una garanzia per chi compra.
Gli acquisti, anche quelli fraudolenti, non passano inosservati. Facendo passare il lettore vicino alla carta, il dispositivo ha **emesso un sonoro «bip» e abbiamo ricevuto un Sms di conferma** dell'avvenuto pagamento.



Quindi è possibile rubare soldi dalle nostre carte/smartphone solo con il tocco di un Pos? **Sì, teoricamente è possibile**, su importi relativamente piccoli e solo su carte di credito. Il punto fondamentale è che **ci si può accorgere del furto istantaneamente** grazie al segnale acustico del dispositivo e grazie all'sms inviato al numero associato.
Per poter usare un Pos e quindi portare a termine il colpo, comunque, il malintenzionato deve caricare nel sistema i suoi documenti che possono far risalire alla sua identità in relativamente poco tempo. Uno strumento in più a difesa del consumatore e del cittadino.

I portafogli con il «blocco» Rfid/Nfc funzionano?
In diverse catene di elettronica e online è possibile acquistare portafogli le custodie Rfid/Nfc (le cosiddette **blocking cards**), vendute per proteggere le proprie carte di credito da questi furti o dalla clonazione delle carte. In breve, tali custodie creerebbero un «disturbo» per schermare la carta di credito.
Qualcosa che in realtà accade già quando una carta di credito è vicina ad un'altra, oppure al passaporto o altre tessere, carte fedeltà, etc. **Un metodo suggerito dagli esperti è infatti proprio**

quello di tenere nel portafogli due carte, l'una appoggiata all'altra, in modo da creare un'interferenza che non permette agli eventuali «strusciatori» di far funzionare il Pos.
In sostanza, questi sistemi non sono utili e oltre a non funzionare per lo scopo sono anche uno spreco di soldi, almeno stando **al parere** degli esperti.
Nel 2023 un gruppo di ricercatori tutto italiano ha pubblicato uno studio sul tema su **arxiv**. I ricercatori hanno provato 11 blocking cards a protezione delle carte di credito, che sono state messe a contatto con un dispositivo per sottrarre i dati contenuti nelle carte di pagamento. Ben 8 sistemi di sicurezza di queste carte sono stati bypassati, perché impiegavano una tecnologia obsoleta o facilmente eludibile e sono quelle che generavano un «rumore bianco». Leggermente più efficaci quelle dotate di una barriera metallica, **ma la protezione è comunque parziale**. Lo studio è stato comunque utile per pensare ad un sistema di protezione alternativo e reso open source, in modo che potesse essere preso in considerazione dai produttori per assicurare una maggiore sicurezza ai clienti finali.

Attenti allo skimmer

Un capitolo a parte sono invece gli skimmer, dispositivi applicati sui Pos o agli sportelli dove si preleva denaro. Si tratta di strumenti che **possono clonare la carta**. Anche in questo caso serve un ulteriore passaggio, che è quello di **recuperare il Pin degli utenti**. Generalmente viene usata una telecamera nascosta per registrare i movimenti delle dita. O, in alternativa, un ulteriore dispositivo inserito fisicamente nel macchinario per memorizzare il codice digitato sul tastierino. **Una misura che non serve per gli smartphone** e che comunque richiede l'inserimento fisico della carta nella fessura dello skimmer.