

Uno scontrino lasciato al bancomat può svuotare il conto: cosa sta succedendo in Sicilia

Autore: Walter Giannò

Data: 25 Febbraio 2026



Nel 2026 una frode semplice, basata su uno **scontrino cartaceo lasciato al bancomat**, si sta diffondendo nel Sud Italia con segnalazioni in Sicilia, nel Palermitano, nel Catanese e nel Siracusano. La cosiddetta “**truffa dello scontrino bancomat**” è già stata documentata in Puglia e ora registra casi anche sull'isola. Il meccanismo non sfrutta falle informatiche sofisticate, ma informazioni parziali stampate sulle ricevute di prelievo.

A lanciare l'allarme è **Gabriele Urzì**, dirigente nazionale **Fabi** e rappresentante salute e sicurezza **Fabi Palermo**, esperto in sicurezza bancaria, che da anni monitora l'evoluzione delle frodi legate ai servizi finanziari.

“Sembra incredibile che nel 2026 si possa ancora cadere vittima di una truffa basata su uno scontrino cartaceo, ma purtroppo accade. Anche in Sicilia abbiamo ricevuto segnalazioni di utenti contattati da finti operatori bancari che utilizzavano dati ricavati dagli scontrini lasciati nei bancomat. Il fenomeno è stato portato all'attenzione della cronaca da truffa.net, portale

specializzato nell'analisi delle frodi digitali e finanziarie, che ha descritto le modalità operative dei truffatori e l'espansione del raggio nel Sud Italia”.

Come funziona la truffa dello scontrino bancomat

Il raggio parte da un gesto apparentemente irrilevante: lasciare lo scontrino del prelievo nello sportello automatico o nei pressi dell'ATM.

Secondo quanto ricostruito, i truffatori recuperano le ricevute e agiscono su due livelli.

Prima fase: incrocio dei dati. Le informazioni riportate sullo scontrino vengono abbinate ad altri dati già in possesso dei malintenzionati per tentare di ricostruire l'identità del titolare del conto.

Seconda fase: contatto diretto con la vittima. Fingendosi operatori bancari, utilizzano i dettagli stampati sulla ricevuta per rendere credibile la telefonata.

I dati presenti sullo scontrino possono includere:

- Data e orario dell'operazione
- Importo prelevato
- Ultime cifre della carta
- Saldo residuo
- Tipo di operazione effettuata

Singolarmente, questi elementi non consentono di accedere al conto o svuotarlo. Ma citati durante una telefonata, trasformano la truffa in un contatto apparentemente legittimo.

Il ruolo del “social engineering”

Il meccanismo – [spiegato su Truffa.net](#) – si basa su tecniche di “social engineering”, che consistono nell'utilizzo, da parte dei pirati informatici, di metodi che hanno come scopo quello di ottenere informazioni personali tramite l'inganno.

Il truffatore chiama, si presenta come operatore della banca e cita dati reali: l'importo dell'ultimo prelievo, il giorno, l'orario. A quel punto chiede conferma di ulteriori informazioni “per sicurezza”.

La credibilità si costruisce su dettagli veri. La vittima, rassicurata dalla precisione dei riferimenti, può arrivare a comunicare:

- Codici di accesso
- Password temporanee
- Codici OTP ricevuti via sms
- Dati completi della carta

Secondo quanto segnalato, il punto debole non è la tecnologia bancaria ma la componente psicologica. I truffatori sfruttano paura e fiducia. Bastano pochi elementi autentici per convincere, in particolare le persone anziane, che si tratti realmente della banca.

Le aree coinvolte e l'espansione del fenomeno

Il fenomeno è stato inizialmente documentato in Puglia. Le segnalazioni si sono poi estese alla Sicilia, con casi riferiti nelle aree di Palermo, Catania e Siracusa.

La diffusione nel Sud Italia è stata descritta da truffa.net, portale specializzato nell'analisi delle frodi digitali e finanziarie, che ha ricostruito le modalità operative e l'espansione territoriale del raggio.

Non si tratta di episodi isolati ma di una dinamica che sfrutta comportamenti quotidiani e ripetuti.

Perché lo scontrino è un rischio reale

Lo scontrino di un bancomat non riporta il numero completo della carta né il codice segreto. Tuttavia contiene dati sensibili che, combinati con altre informazioni reperibili online o tramite precedenti violazioni, possono facilitare l'attacco.

La sequenza tipica descritta è questa:

1. Recupero della ricevuta lasciata allo sportello
2. Ricerca di informazioni aggiuntive sulla vittima
3. Telefonata con citazione di dettagli reali
4. Richiesta di ulteriori dati "di verifica"
5. Accesso al conto tramite credenziali fornite dalla vittima

La forza del raggio sta nella coerenza narrativa costruita dal truffatore.

Il meccanismo

Fase	Azione del truffatore	Obiettivo
Recupero	Raccoglie lo scontrino lasciato all'ATM	Ottenere dati parziali
Incrocio dati	Abbina informazioni già in possesso	Identificare il titolare
Contatto	Si finge operatore bancario	Ottenere fiducia
Manipolazione	Usa social engineering	Farsi comunicare dati sensibili
Accesso	Utilizza credenziali ricevute	Entrare nel conto corrente

FAQ

Lo scontrino del bancomat permette di accedere direttamente al conto?

No, ma fornisce dati che rendono credibile la telefonata del truffatore.

Dove si sono registrate le segnalazioni?

In Puglia e in Sicilia, in particolare nel Palermitano, Catanese e Siracusano.

Qual è il punto debole sfruttato dai truffatori?

La componente psicologica e la fiducia della vittima.

Chi ha lanciato l'allarme?

Gabriele Urzì, dirigente nazionale Fabi ed esperto in sicurezza bancaria.

Riferimento articolo: <https://www.siciliafan.it/truffa-scontrino-bancomat-sicilia-2026-segnalazioni/>

Generato il 16/04/2026