



# Postepay ATM Scam: The Guide to Avoid Falling into the Trap

**Autore:** Francesco Zinghini | **Data:** 15 Novembre 2025

---

In the landscape of digital payments, the Postepay card has established itself in Italy as an almost traditional tool, combining the convenience of a prepaid card with the vast network of Poste Italiane. However, its immense popularity has also made it a prime target for scammers. One of the most insidious and psychologically sophisticated frauds is the **fake Postepay top-up scam**, which preys on victims' naivety and a distorted understanding of ATM procedures. This scheme doesn't rely on complex hacking techniques but on social engineering, turning the seller of a used item into the victim of a theft.

This article analyzes the mechanics of this scam in detail, explaining how criminals manipulate people and why this technique is so effective. It will provide practical advice and warning signs to recognize the fraud attempt and will outline the steps to take if you fall into the trap, from reporting it to the authorities to requesting a refund. The goal is to provide a comprehensive guide for self-defense, raising awareness about a criminal phenomenon that exploits trust and a lack of familiarity with banking procedures.

## How the Fake Top-Up Scam Works

The fake Postepay top-up scam is a deception that almost always occurs in the context of online sales between private individuals on platforms like Subito.it or Facebook Marketplace. The mechanism is as simple as it is diabolical: the scammer doesn't steal data with phishing techniques but convinces the victim

to send them money voluntarily, making them believe they are receiving a payment. The fraud is based on a fundamental misunderstanding: passing off an outgoing top-up transaction as an incoming credit, exploiting the victim's confusion at the ATM.

## **The Trap is Set Online**

It all begins when a person lists an item for sale on a classifieds website. The scammer, posing as a very interested and often hurried buyer, contacts the seller. After a brief and superficial negotiation, they declare their intention to close the deal immediately and offer to pay right away via a "Postepay top-up." To make it more credible, the fraudster feigns urgency, pushing the victim to go to a Postamat or any enabled ATM without delay. This rush is a calculated psychological tactic to prevent the victim from having time to think or ask for advice.

## **Deceptive Instructions at the ATM**

Once the victim is in front of the ATM, the scammer guides them step-by-step over the phone. The instructions are precise and aimed at creating confusion. The seller is asked to insert their card, select the "Postepay Top-Up" (Ricarica Postepay) option, and enter the agreed-upon amount. The crucial step occurs when the scammer provides a Postepay card number to enter, claiming it is an "order code" or a "transaction number" needed to *receive* the money. In reality, that is the scammer's card number. The victim, convinced they are collecting a sum, is instead topping up their tormentor's card.

## Why This Scam Is So Effective

The success of this fraud lies not in technology, but in psychological manipulation. Scammers are skilled at creating a context of trust and urgency that causes the victim to lower their defenses. They exploit people's natural tendency to trust those who appear polite and decisive, combined with an often superficial knowledge of banking operations. The Mediterranean culture, based on interpersonal relationships and a certain informality, can unintentionally favor this type of manipulative approach, where a spoken promise over the phone takes on an almost contractual value.

### Social Engineering and the Trust Factor

Social engineering is the art of manipulating people into performing specific actions or divulging confidential information. In this case, the scammer builds a credible persona: the ideal buyer, decisive and ready to pay. The phone conversation is the key tool: the human voice conveys a greater sense of security than a written message. The criminal uses reassuring and professional language, guiding the victim with calm and competence, dispelling any doubts. The urgency they impose serves to create psychological pressure, pushing the victim to make mistakes they wouldn't make with a clear mind.

### The Confusion Between “Top-Up” and “Cardless Withdrawal”

The heart of the deception lies in a terminological misunderstanding. To receive money on a Postepay card, it is **never necessary to go to an ATM**. Payments are received automatically. The “top-up” operation is exclusively for *sending* money to another card. Scammers exploit the mistaken idea that collecting a payment requires an active step by the seller. They deliberately

confuse the top-up operation with cardless withdrawal procedures or other complex features, preying on many users' lack of familiarity with advanced ATM options.

## **How to Protect Yourself from the Postepay Top-Up Scam**

The most effective defense against this type of fraud is awareness. Knowing how the scam works and paying attention to some unmistakable signs can make the difference between a successful sale and a financial loss. The fundamental rule is simple: to receive a payment, you should never perform operations at an ATM following instructions from a third party. Caution and the use of secure payment methods are the best weapons for protection.

### **Warning Signs Not to Be Ignored**

The first red flag is being asked to get paid through a procedure that involves going to an ATM. If a supposed buyer insists on this method, it is almost certainly a scam attempt. Other signs include excessive haste to close the deal and the request to stay on the phone during the ATM transaction. You should be wary of anyone who provides "codes" or "order numbers" to be entered on the top-up screen. If you have any doubts about the procedure, it's better to stop the transaction and, if necessary, get information through official Poste Italiane channels, such as the toll-free number 803.160.

### **The Golden Rules for Secure Payments**

For online sales between private individuals, it is essential to prioritize traceable and secure payment methods that protect the seller. A bank transfer is one of the most reliable options, as it leaves a clear record of the

transaction. Systems like PayPal (with seller protection) also offer a good level of security. It is important to remember that a Postepay top-up is an instant and, unlike a bank transfer, non-revocable operation. If a payment fails, you might encounter an issue like a [failed Postepay top-up](#), but this never requires you to go to an ATM to resolve the situation. Furthermore, never share sensitive data like your PIN or your card's security codes.

## What to Do If You've Fallen into the Trap

Realizing you've been scammed is a frustrating experience, but it's crucial to act quickly and clearly to limit the damage and initiate the correct procedures. Time is a critical factor. The first thing to do is secure your card and gather all possible evidence to file a report. Although recovering the money is not guaranteed, reporting the incident is an essential step both to attempt a refund and to help law enforcement combat these criminal phenomena.

## Steps to Follow Immediately After the Scam

As soon as you realize the fraud has occurred, immediately contact Poste Italiane customer service to **block your card** and prevent further unauthorized transactions. Gather all useful information: the scammer's phone number, screenshots of conversations, the online ad, and any other details related to the transaction. These elements will be crucial for the report. In case of suspicious charges, it's important to know how to act, as explained in the guide on what to do in case of [suspicious charges on Postepay](#).

## Filing a Report and Refund Possibilities

With all the evidence collected, go as soon as possible to a Postal Police office or a Carabinieri station to **file a formal complaint**. This act is a mandatory requirement to initiate any dispute procedure. Subsequently, with a copy of the complaint, you can submit a chargeback form to Poste Italiane to request a refund. Unfortunately, since the top-up is a voluntary operation, getting the money back is difficult, but not impossible. Filing a report is also crucial for similar cases, such as that of a [cloned Postepay card](#).

## Conclusion

The fake Postepay top-up scam is a prime example of how innovation in digital payments can be exploited by old deception techniques based on psychological manipulation. The Postepay card, a symbol of modernization within the Italian postal tradition, unintentionally becomes a tool for fraud. The best defense lies in education and awareness: understanding that *no credit operation requires an active step at an ATM* is the first step to protecting yourself. It is essential to be wary of unusual procedures and rushed requests, always favoring secure and traceable payment channels. Always reporting any scam attempt is a civic duty that helps make the digital ecosystem a safer place for everyone, protecting the foundation of trust that underlies every exchange, whether traditional or innovative.

## Frequently Asked Questions

### How exactly does the fake Postepay top-up scam work?

The scam typically takes place during an online sale. The scammer, posing as a buyer, contacts the seller and offers to pay via a Postepay 'top-up.' They then convince the victim to go to a Postamat or other ATM and guide them by phone

through a transaction that, unbeknownst to them, is not an incoming credit but an outgoing top-up. In practice, the seller is induced to enter the scammer's card number and an amount, effectively making a payment to the fraudster instead of receiving one.

### **What are the signs to recognize a scam attempt?**

The first red flag is the request to go to an ATM to receive a payment. A legitimate buyer does not need the seller to perform any operations at the ATM. Other signs include insistence on guiding the transaction over the phone and the use of ambiguous terms like 'order number' to disguise the card number to be topped up. Always be wary of anyone who asks you to perform unconventional or unfamiliar payment procedures.

### **What should I do if I realize I've been scammed?**

The first thing to do is to immediately block your card to prevent further damage by contacting the Poste Italiane toll-free number (800.00.33.22 from Italy). Next, it is crucial to gather all evidence (chats, the scammer's phone number, transaction details) and file a report with law enforcement, such as the Postal Police. With a copy of the report, you can submit a dispute form to Poste Italiane to attempt to get a refund.

### **Is it possible to recover the money lost in this scam?**

Recovering the money is difficult, but not impossible. A Postepay top-up is an immediate transaction, and the scammer can withdraw the sum almost instantly. For this reason, speed is crucial. Immediately filing a report and starting the dispute process with Poste Italiane are essential steps. However, the success of the recovery is not guaranteed and depends on many factors, including how quickly you act.

## **Why do scammers insist on using an ATM?**

Scammers exploit some people's lack of familiarity with the operations available at ATMs. By guiding the victim over the phone, they can easily confuse them, disguising an 'outgoing top-up' operation (a payment) as a procedure to 'receive a credit.' The ATM environment, combined with the psychological pressure exerted by the scammer, induces the victim to follow incorrect instructions that they would not follow under normal conditions.