

# [Il Commissariato di Orvieto denuncia tre persone per truffe online](#)

scritto da Redazione | 4 Agosto 2021



Sono **tre** gli episodi di **truffa online** scoperti dagli investigatori della **Polizia di Stato di Orvieto**, grazie ad accurate **indagini**, avviate alcuni mesi fa dalla squadra anticrimine del **Commissariato di Pubblica Sicurezza**, dopo che le vittime dei raggiri si sono rivolte agli agenti raccontando di come sono cadute nella rete di persone senza scrupoli, che questa volta però sono state identificate e denunciate per truffa.

Il primo episodio risale a fine settembre, quando un **45enne di Orvieto** si è presentato negli uffici del Commissariato di Piazza Cahen per **sporgere denuncia** contro ignoti, in quanto aveva ricevuto una **bolletta del Servizio Elettrico Nazionale** per un importo di **767,01 euro**, relativa ad una fornitura intestata a lui ed alla moglie deceduta. Quando l'uomo aveva **chiamato il servizio clienti**, aveva scoperto che **a nome della moglie defunta** risultavano intestate altre **nove utenze**, con contratti attivati in varie parti d'Italia, prevalentemente in **Piemonte** e uno in **Campania**. Dalle indagini effettuate, è emerso che la **maggior parte dei residenti** agli indirizzi presenti nei contratti erano **estranei** alla vicenda, mentre, **due persone** - padre e figlio - rispettivamente di 53 e 24 anni, residenti in **provincia di Caserta**, hanno fornito versioni contrastanti in merito all'attivazione del contratto dell'energia elettrica, **contratto** che poi è risultato essere stato **registrato** in modo **fraudolento**, motivo che ha portato alla denuncia dei due.

Nel secondo caso, ad essere stato truffato è un **uomo di 59 anni** residente a **Castel Viscardo**, che ha versato la somma di **250 euro** su una **carta Sisal Pay Money** per l'**acquisto** di un **cellulare** che non ha **mai ricevuto**. L'uomo aveva visto il telefonino sul **sito online Marketplace di Facebook**, messo in **vendita da una donna** sul suo profilo e aveva telefonato per accordarsi sulle modalità di acquisto del cellulare; gli veniva chiesto di fare una **ricarica di 250 euro** su una carta Sisal Pay Money e gli veniva **inviata - tramite foto** - una copia della **ricevuta di Poste Italiane** dell'avvenuta spedizione (spedizione **mai avvenuta** in verità). Le **indagini** hanno permesso di risalire all'**intestatario della carta Sisal Pay**, un **36enne** residente a **Pompei (NA)**, che risultava anche intestatario della **scheda telefonica** usata per la transazione; l'uomo, con **precedenti penali**

per reati simili, è stato denunciato, mentre gli accertamenti volti ad identificare la **donna del profilo Facebook** hanno dato esito **negativo**.

Il **terzo episodio** è sicuramente quello più efferato, in quanto perpetrato ai danni di una **signora non completamente autosufficiente**, alla quale è stato prosciugato il **conto alle Poste**. La signora ha riferito agli agenti del **Commissariato di Pubblica Sicurezza** di Orvieto che a **fine marzo** aveva ricevuto un **SMS**, da un numero sconosciuto, in cui le si inviava un **link da scaricare** per fare un **aggiornamento** sul proprio conto corrente postale. Dato che la donna, una **63enne orvietana**, aveva davvero un conto alle Poste, ha tentato di **clickare il link**, **senza** però riuscire ad **aprirlo**. Immediatamente **dopo**, aveva ricevuto una **telefonata da un numero privato** e una voce femminile, dopo averle assicurato di essere **una dipendente delle Poste**, le aveva detto che avrebbe **provveduto lei a fare gli aggiornamenti** necessari, chiedendole di **fornirle** telefonicamente i **codici** di accesso al conto personale, cosa che la signora faceva. Controllando il conto personale, avendo realizzato che potesse trattarsi di un raggiro, aveva riscontrato che subito **dopo la telefonata**, con la **donna** che si era **spacciata per un'impiegata delle Poste**, erano stati effettuati **due addebiti di 2.990 euro** ciascuno e poco prima che la signora riuscisse a bloccare il conto, un **terzo** addebito per un importo di **2.860 euro**. Gli **accertamenti** effettuati hanno portato all'individuazione di un **numero utilizzato** per le operazioni fraudolente di **phishing**, il 3314180xxx, intestato ad un **20enne** della **provincia di Caserta**, che è stato rintracciato e che, fornendo spiegazioni non plausibili in merito alla documentazione presentata per l'intestazione della SIM card, è stato **denunciato per truffa**; le indagini sono ancora in corso per identificare gli intestatari delle **tre** diverse carte **PostePayEvolution**, sulle quali sono **confluiti i tre addebiti**.

La **Polizia di Stato**, già da anni, ha avviato delle campagne di informazione, sia sui social, che sulla stampa, per **mettere in guardia** da truffe e raggiri, attuati tramite contatti telefonici o via internet, come il **phishing** (una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti che si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli).

La Polizia di Stato avverte che i **cybertruffatori** agiscono anche tramite invio di sms che contengono dei falsi messaggi di richiesta di aggiornamenti o di acquisti on line che invitano a cliccare su dei link, contenuti nel messaggio dai quali viene scaricato un **file che, installato sul cellulare**, permette ai malfattori di **accedere al dispositivo** ottenendone il controllo e di impossessarsi dei dati sensibili. Pertanto, **password, dati delle carte, codici Otp, Pin, credenziali, chiavi di accesso all'home banking o altri codici personali** entrano a far parte della banca dati dei truffatori del web. Si tratta del cosiddetto fenomeno di **smishing**, termine che deriva dall'unione delle parole sms e phishing, dove l'ultimo termine indica la "pesca" dei dati. La Polizia di Stato invita a verificare le informazioni sul sito ufficiale dell'ente che invia il messaggio, evitando di utilizzare il link contenuto ma digitandone il nome direttamente sulla barra degli indirizzi (Url). In caso di sospetti si può effettuare una segnalazione sul sito <https://www.commissariatodips.it/> Commissariato di PS online: sportello per la sicurezza degli utenti del web, un commissariato di P.S. online al passo con i tempi dei social network che permette di avere delle risposte immediate, in tempo reale, per evitare di cadere nelle tante trappole che ci sono online.