



Verbraucherzentrale Südtirol
Centro Tutela Consumatori Utenti

Die Stimme der VerbraucherInnen
La voce dei consumatori

Centro Tutela Consumatori Utenti

Via Dodiciville 2

39100 Bolzano

Tel. 0471 975597

info@verbraucherzentrale.it

Pagamenti digitali

Gio 10/06/2021 - 10:15

Truffa con password "usa e getta"

Il Centro Europeo Consumatori (CEC) e il Centro Tutela Consumatori Utenti (CTCU) hanno recentemente ricevuto numerose segnalazioni di frodi che, pur differendo leggermente nella loro esecuzione, avevano tutte una cosa in comune: le persone truffate credevano tutte di avere a che fare con una banca o una società di carte di credito.

Classifichiamo sempre i messaggi e le chiamate che provengono da banche o società di carte di credito come particolarmente rilevanti e, di solito, li consideriamo automaticamente seri e affidabili, perché: "Viene da una banca!".

Così ha fatto anche la signora Rossi, che ci ha segnalato quanto segue:

"Ho ricevuto un SMS che mi chiedeva di contattare un Numero Verde per indagare su un'irregolarità relativa alla mia carta di credito. Durante la conversazione, il mio interlocutore, che si spacciava per un dipendente della società della mia carta di credito, mi ha fatto consegnare il codice che avevo appena ricevuto via SMS. Quindi ho comunicato il codice, ritrovandomi in questo modo ad acconsentire a un addebito di oltre 1000 euro".

Attenzione alle truffe OTP:

La signora Rossi è stata vittima di una delle tante cosiddette "truffe OTP". OTP sta per "One-Time-Password". Si tratta di un codice spesso richiesto per completare la transazione per i pagamenti digitali con carta di credito od online banking. Viene inviato via SMS o generato tramite altri sistemi solo al momento del pagamento. Si ha bisogno di tali OTP solo se si vogliono effettuare delle spese, non per ricevere denaro o effettuare controlli.

*"In relazione a tali OTP c'è un principio che si dovrebbe sempre rispettare per non cadere in una trappola: **queste password non devono mai essere trasmesse**", spiega **Gunde Bauhofer**, direttrice del CTCU. Indipendentemente dal fatto che siano stati apparentemente inviati dalla persona con cui si stava parlando, a prescindere dalla persona con cui si sta parlando, scrivendo, inviando SMS o messaggi su Whatsapp: **le OTP***

non vanno inoltrate. *"Nessuna banca, società di carte di credito o altro istituto di fiducia le chiederà: l'unico luogo in cui si utilizza l'OTP è il sito, già aperto precedentemente, usato per effettuare il pagamento degli acquisti online, o la pagina dell'online banking"*, conferma **Julia Rufinatscha**, esperta di commercio elettronico del Centro Europeo Consumatori Italia.

Molti altri avrebbero reagito come la signora Rossi se si fossero trovati in una situazione simile. Eppure ci sono passaggi essenziali nella sua storia che sarebbero andati diversamente se in precedenza avesse ricevuto i seguenti suggerimenti:

- Quando si contatta una società di carte di credito o una banca, non bisogna fare mai affidamento sui numeri di telefono trovati sui social media o sui motori di ricerca, dati via SMS o WhatsApp. Prima di comporre il numero per la chiamata, è bene **controllarne sempre prima la veridicità esclusivamente sul sito ufficiale della banca o dell'istituto di carta di credito.**
- Non cliccare mai su link che affermano di provenire dalla banca o dalla società della carta di credito: possono portare a un addebito fraudolento.
- **Controllare** sempre il **contenuto dell'SMS** che si riceve e non inserire mai la combinazione di numeri fornita senza aprire l'SMS.
- Assumere che le banche e i fornitori di servizi finanziari **non chiedono mai codici personali completi o numeri di carta** via SMS o per telefono.
- Se si diventa vittima di una frode OTP, presentare un **reclamo al proprio fornitore di servizi finanziari.**

Maggiori informazioni al link: <https://www.euroconsumatori.org/it/phishing>