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

Vittima di phishing ottiene risarcimento di 13.700 euro

Gio 29/05/2025 - 09:59

Successo del CTCU davanti all'Arbitro Bancario Finanziario
Attenzione agli investimenti online sui social-media

Il signor Bruno (nome di fantasia) aveva ricevuto una chiamata da un numero telefonico che aveva attribuito alla sua banca. A chiamare, tuttavia, era un truffatore che gli aveva chiesto di apportare modifiche al sistema di autenticazione della sua area riservata. L'interessato dichiarava di aver effettuato l'accesso all'applicazione, ma di non essere più stato in grado di risalire a ciò che aveva fatto nell'applicazione, seguendo le “istruzioni” del truffatore. Quando il sig. Bruno aveva notato che dal suo conto era stato effettuato, a sua insaputa, un bonifico di 13.700 euro, si era immediatamente reso conto di essere stato ingannato; purtroppo il denaro era ormai sparito. La vittima si era quindi rivolta al CTCU, che, in seguito ad un iniziale reclamo infruttuoso, aveva quindi sottoposto il caso (di phishing) all'Arbitro Bancario Finanziario.

Che cos'è il “phishing”?
Il “phishing” è una tipologia di truffa, nella quale le persone vengono contattate in modo mirato tramite e-mail, messaggi, telefonate oppure altri canali di comunicazione. Lo scopo di questi “agganci” è quello di convincere le persone coinvolte a compiere una determinata azione, ad esempio, a rivelare informazioni sensibili come propri dati finanziari, propri dati di accesso ad aree riservate oppure altre informazioni personali.
Nel corso di queste frodi, i truffatori non attaccano direttamente i sistemi di sicurezza (ad esempio, di determinati istituti bancari), ma si avvalgono invece di tecniche di ingegneria sociale verso le potenziali vittime: attraverso sottili manipolazioni psicologiche e informazioni ingannevoli, e grazie anche al supporto tecnologico (ad esempio, e-mail, messaggi o telefonate fraudolenti), fingono di essere operatori di “istituzioni” affidabili, quali istituti bancari, fornitori di carte di credito o altro ancora. In

questo modo, inducono le vittime a cliccare su link che conducono a siti fasulli, a scaricare file dannosi oppure a rivelare informazioni riservate come i dati di accesso al proprio conto corrente o alla propria carta di credito. I truffatori, ottenute le informazioni necessarie, possono poi effettuare, indisturbati, transazioni bancarie dai conti delle vittime.

Autenticazione a due fattori

I legislatori europei e nazionali hanno stabilito che la cd. “autenticazione a due fattori” deve essere effettuata per ogni transazione o operazione bancaria a distanza, che potrebbe potenzialmente causare un danno economico al cliente. Nel caso in cui la banca non effettui l'autenticazione a due fattori, il cliente ha diritto al rimborso completo della perdita finanziaria subita.

Che cos'è l'autenticazione a due fattori?

L'autenticazione a due fattori è una procedura di sicurezza in cui l'accesso a un sistema o l'esecuzione di una transazione sono consentiti solo se vengono verificati almeno due fattori di riconoscimento indipendenti fra loro, permettendo così di verificare con sicurezza l'identità dell'utente.

I due fattori possono appartenere alle seguenti categorie:

1. **conoscenza:** qualcosa che solo l'utente conosce, ad esempio, una password o un PIN;
2. **possesso:** qualcosa che solo l'utente possiede, come, ad esempio, un dispositivo smartphone, una carta bancaria o un generatore di OTP;
3. **biometria:** qualcosa che solo l'utente è, ad esempio un'impronta digitale, il riconoscimento facciale oppure quello vocale.

Come si è pronunciato l'ABF nel caso in questione?

In questo caso specifico, la banca non è stata in grado di dimostrare l'utilizzo dell'autenticazione a due fattori al momento dell'accesso del truffatore all'online banking della vittima. Se manca infatti la prova dell’autenticazione forte anche solo per una delle fasi del processo di pagamento, cioè in questo caso già al momento dell'accesso al sistema, la banca può essere ritenuta responsabile del danno subito dal proprio cliente.
Poiché la banca non è stata in grado di fornire tale prova, l’ABF ha dato ragione al cliente e ha imposto alla banca di risarcire allo stesso l'intera perdita da questi subita.

"Questo caso si è concluso positivamente per il cliente. Tuttavia, non tutte le vittime di truffe online possono aspettarsi sempre decisioni altrettanto favorevoli", afferma Gunde Bauhofer, direttrice del CTCU. "Nel caso in cui la banca sia in grado di dimostrare che è stata effettuata una cosiddetta autenticazione forte, cioè a due fattori, l’ABF potrebbe prendere, infatti, anche una decisione diversa,

sfavorevole per il consumatore".

Cosa fare nel caso siate stati vittime di “phishing”?

- Far bloccare immediatamente la carta o il conto corrente al proprio istituto bancario;
- sporgere denuncia alle autorità di pubblica sicurezza (polizia/carabinieri/guardia di finanza);
- segnalare subito l’accaduto al fornitore di servizi finanziari, chiedere di annullare le eventuali transazioni illecite compiute dai malfattori; chiedere il rimborso delle somme sottratte (allegando copia della denuncia presentata).
- Nel caso in cui il fornitore di servizi finanziari non dovesse rispondere alla vostra richiesta oppure dovesse rispondere, rifiutando il rimborso, è poi possibile presentare un ricorso all'organo arbitrale della Banca d'Italia, l'Arbitro Bancario Finanziario (per informazioni si può consultare il seguente link: www.arbitrobancariofinanziario.it. Il CTCU offre assistenza per la redazione di questo tipo di ricorso.

Aumenta il numero di richieste di informazioni sulle frodi nel commercio online

Negli ultimi mesi, il Centro Tutela Consumatori Utenti (CTCU) ha ricevuto un numero crescente di richieste di assistenza e informazione su casi di frode nel commercio online. Nei casi noti, il primo contatto è avvenuto solitamente tramite social network, come ad esempio facebook, instagram o altro social-media, e per convincere la vittima vengono mostrati dei video in cui personaggi pubblici molto noti sembrano consigliare degli investimenti. Questi video non riproducono situazioni reali, ma vengono realizzati con l'aiuto dell'intelligenza artificiale e, a volte, sembrano molto credibili.
Una volta stabilito il contatto iniziale, le vittime vengono invitate a effettuare investimenti, spacciati come redditizi, tramite messaggi personali, spesso via WhatsApp. In realtà si tratta di pagamenti che non vengono assolutamente poi investiti in qualche tipo di operazione finanziaria, ma che finiscono direttamente nelle tasche dei truffatori e quindi spariscono.
Per questo motivo, il CTCU consiglia vivamente di stare alla larga da simili proposte di investimento offerte tramite i social-network. Le truffe segnalate al CTCU ammontano talvolta anche a molte migliaia di euro, superando addirittura in taluni casi somme di 100.000 euro e oltre.

I consulenti del Centro Tutela Consumatori Utenti sono a disposizione per fornire informazioni e assistenza in merito (tel. 0471-975597).