

Phishing, attenzione alla truffa dei finti recuperi crediti sanità. Ecco cosa fare

Data: 10 novembre 2025 | Autore: Redazione

Dettagli Posizione Debitoria e Pagamento

Indicazioni Obbligatorie per il Pagamento - Bonifico Bancario

L'importo totale da saldare è di **€ 40,10** entro e non oltre la data indicata nell'email.

L'importo include sanzioni amministrative e spese di comunicazione. Utilizzare i seguenti dati per effettuare il bonifico bancario. L'uso corretto della causale di pagamento è essenziale per la corretta registrazione del versamento e la chiusura della Sua pratica.

Beneficiario	Importo
[REDACTED]	€ 40,10
IBAN	BIC/SWIFT
[REDACTED]	[REDACTED]

[Copia](#)

CAUSALE DI PAGAMENTO

Saldo Pratica 460446 [Copia](#)

ATTENZIONE: Il mancato pagamento entro la scadenza indicata nell'email di avviso comporterà l'avvio delle procedure legali di recupero coattivo del credito, con aggravio di spese a Suo carico.

Phishing in Lombardia: attenzione alla truffa delle false richieste di pagamento

Nuova campagna di phishing contro i cittadini: email con finti recuperi crediti per prestazioni sanitarie

È in corso una campagna di phishing che sta colpendo numerosi cittadini della Regione Lombardia, attraverso email truffaldine legate a presunti mancati pagamenti di prestazioni sanitarie.

Queste comunicazioni arrivano da una sedicente società di recupero crediti e riportano come oggetto la dicitura: "Richiesta di saldo debito – nome e cognome".

Perché queste email sono così insidiose

La truffa è particolarmente pericolosa perché le email includono un elenco di prestazioni sanitarie e ricette mediche realmente emesse dai medici curanti dei pazienti. Questo dettaglio crea un'apparenza di autenticità che spinge molti cittadini a fidarsi e a procedere al pagamento.

L'importo richiesto è mediamente intorno ai 40 euro e il versamento deve essere effettuato su un

conto corrente estero, spesso identificato da un IBAN spagnolo.

Come riconoscere la truffa

- L'ente che invia la comunicazione non è riconducibile ad alcuna azienda autorizzata.
- Il pagamento richiesto non avviene tramite i canali ufficiali della Regione Lombardia o del Sistema Sanitario Nazionale.
- La presenza di un IBAN straniero è un chiaro segnale di frode.

Cosa fare in caso di sospetto phishing

Se ricevi un'email con queste caratteristiche, non effettuare alcun pagamento e non cliccare sui link presenti nel messaggio.

È consigliato segnalare immediatamente l'accaduto alla Polizia Postale, anche attraverso il portale ufficiale: www.commissariatodips.it.

Conclusione

Le truffe online legate al phishing diventano ogni giorno più sofisticate, sfruttando dati reali per ingannare le persone. Per proteggersi è fondamentale diffidare da richieste di pagamento anomale e verificare sempre tramite i canali istituzionali.

Attenzione: è una truffa! Proteggi i tuoi dati e segnala ogni tentativo sospetto.

Articolo scaricato da www.infooggi.it

<https://www.infooggi.it/articolo/phishing-in-lombardia-attenzione-alla-truffa-delle-false-richieste-di-pagamento/148755>