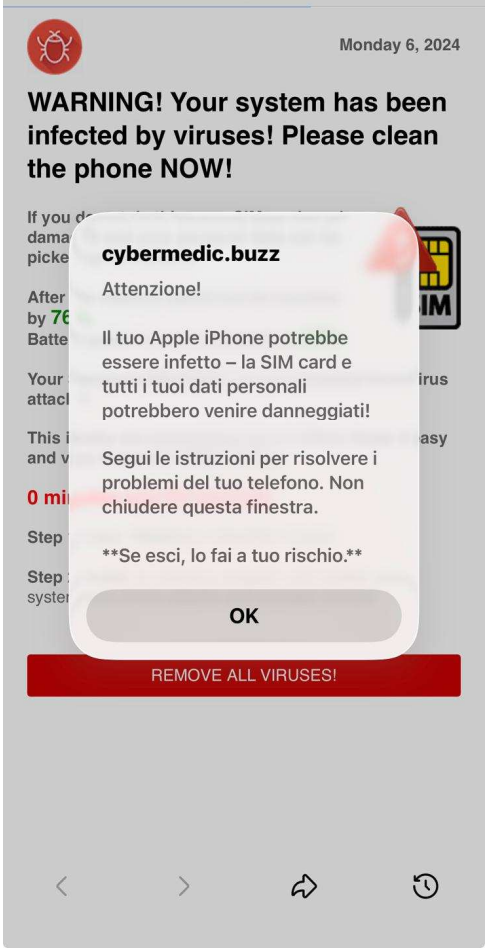

TRUFFA NON CLICCARE MA CHIUDERE LA PAGINA

Si tratta al 100% di una bufala (una truffa o un tentativo di scareware / phishing). Analizzando l'immagine che hai inviato, ci sono elementi inequivocabili che lo dimostrano:Il dominio e la provenienza: La pagina visualizzata proviene da un indirizzo sospetto (cybermedic.buzz) spacciato o aperto all'interno di Facebook, e nessun browser o sistema operativo (iOS) può scansionare l'interno della SIM card o rilevare virus tramite una semplice pagina web. Le tecniche di pressione psicologica: Vengono usati messaggi allarmistici ("WARNING! Your system has been infected!", "Il tuo Apple iPhone potrebbe essere infetto", "Se esci, lo fai a tuo rischio.") tipici delle truffe online per spingere l'utente a cliccare d'istinto su pulsanti come "OK" o "REMOVE ALL VIRUSES!". Come funziona questo inganno: È un classico pop-up JavaScript malevolo o ingannevole generato da un sito web visitato (spesso reindirizzato da banner pubblicitari aggressivi). Serve solo a spaventarti per farti scaricare app inutili/dannose, abbonamenti a pagamento nascosti o per rubare dati personali.Cosa fare adesso:Chiudi immediatamente la scheda del browser (o l'applicazione) da cui proviene la schermata, senza cliccare su "OK" o su altri pulsanti all'interno del pop-nar.Non scaricare nulla di ciò che viene proposto.Per sicurezza, puoi svuotare la cache e i dati di navigazione del browser del telefono.Il tuo iPhone non ha subito alcuna violazione a causa di questa schermata: si tratta unicamente di un avviso falso progettato per intimidire chi naviga.

SOLUZIONE

Per eliminare la cache e liberarsi definitivamente di questi fastidiosi pop-up pubblicitari o truffaldini su iOS (iPhone), la procedura corretta consiste nel pulire i dati di navigazione del browser (solitamente Safari o Chrome) da cui si è aperta quella pagina.

Ecco i passaggi dettagliati da seguire:

1

Chiudi tutte le schede aperte nel browser

Primo passo

Esci dalla pagina della truffa chiudendo la scheda corrente. Se usi Safari, tocca l'icona delle due finestre sovrapposte in basso a destra, quindi chiudi la scheda toccando la "X" o scorrendola via.

Verification: La pagina sospetta non è più visibile tra le schede aperte del browser.

2

lisci la cronologia e i dati dei siti web (Safari)

Impostazioni di iOS

Vai su Impostazioni del tuo iPhone, scorri verso il basso e seleziona Safari. Scorri ulteriormente fino a trovare la voce Cancella dati siti web e cronologia, toccala e conferma l'operazione.

Verification: L'opzione si oscura o risulta azzerata, segno che la cache e i cookie di navigazione sono stati eliminati.

3

Riavvia il dispositivo

Pulizia della memoria temporanea

Tieni premuto il tasto laterale e uno dei tasti del volume finché non compare il cursore di spegnimento, spegni l'iPhone e riaccendilo dopo qualche secondo.

Verification: Il telefono si riavvia correttamente e il sistema ricarica un ambiente pulito senza processi annessi in background.

⚠️ **IMPORTANTE: Non toccare mai nulla**

Se in futuro dovesse ricomparire un avviso simile, ricorda che nessun sito web può rilevare virus reali su iOS. Chiudi subito la scheda del browser senza inserire dati personali né scaricare profili o applicazioni sconosciute.