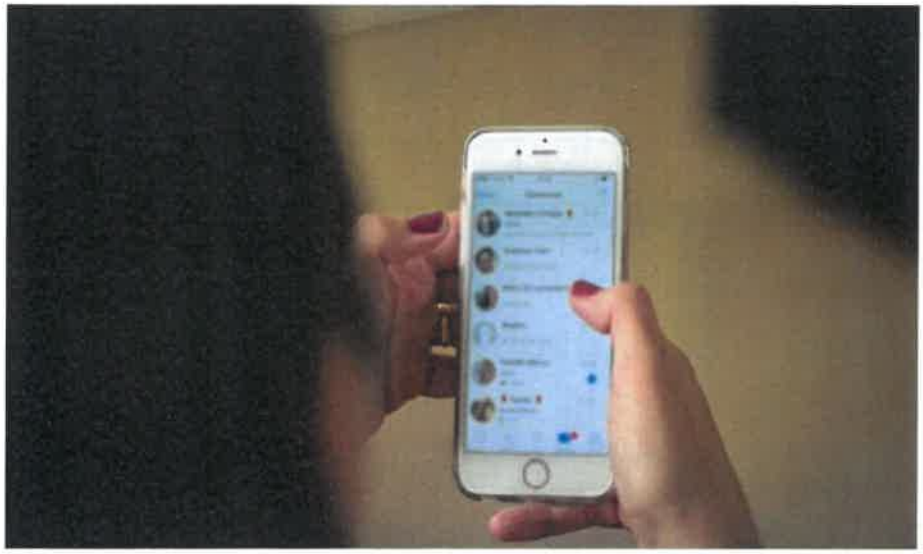
Truffe su WhatsApp, come riconoscere il Ghost Pairing (che arriva dai nostri contatti). «Potresti votare il mio nipote?»

mercoledì 11 febbraio 2026



«Potresti votare per mio nipote?»: si chiama **Ghost Pairing** ed è la **truffa** on-line consente ai cybercriminali di prendere il controllo dell'account **WhatsApp Web** delle vittime per poi causare gravi conseguenze alla privacy e anche al portafoglio. Il messaggio che si riceve - «Ciao! Se non è un problema potresti votare per mio nipote? Manca davvero poco» - è particolarmente insidioso, perché giunge da uno dei contatti della nostra. I I Carabinieri della Cyber Investigation del Comando Provinciale di Napoli stanno seguendo il fenomeno con attenzione, raccogliendo molte denunce.

Come funziona

La truffa - spiegano i militari - ha spesso inizio con la ricezione di un messaggio proveniente da un contatto reale, per esempio un amico, un parente o un conoscente, che invita a votare per una bambina o una giovane ballerina all'interno di un presunto concorso di danza o evento culturale utilizza immagini rassicuranti «Vota», l'utente viene reindirizzato a un popup in cui viene richiesto di autenticarsi tramite WhatsApp, con il pretesto di evitare voti non validi.

Link e codice

Inserendo il proprio numero di telefono e successivamente il codice di verifica che appare sullo schermo, la vittima consente inconsapevolmente ai truffatori di aprire una sessione di WhatsApp Web su un dispositivo controllato dai criminali. A quel punto l'account risulta compromesso: i criminali del web possono leggere i messaggi, impersonare la vittima e inviare richieste di denaro ai suoi contatti, spesso facendo leva su urgentizze improvvise, incidenti o difficoltà personali. Con la stessa modalità, il messaggio-trappola viene poi inoltrato ad altri contatti, alimentando una catena di contagio digitale.

Come difendersi

Questi i consigli utili dei Carabinieri della Cyber Investigation del Comando Provinciale di Napoli per difendersi dalle truffe: Si raccomanda ai cittadini di adottare alcune semplici ma fondamentali precauzioni. - Non cliccare su link sospetti ricevuti tramite messaggi, anche se provengono da contatti conosciuti. - Diffidare da richieste di voto, premi o concorsi che richiedono l'accesso tramite WhatsApp. - Non inserire mai codici di verifica ricevuti via sms o rappresentati a schermo su siti esterni o comunicarli a terzi. - Controllare periodicamente la sezione «Dispositivi collegati» nelle impostazioni di WhatsApp ed eliminare eventuali accessi non riconosciuti. - Attivare la verifica in due passaggi per rafforzare la sicurezza del proprio account.

In caso di dubbio o sospetta compromissione, avvisare immediatamente i propri contatti e rivolgersi alle Forze dell'Ordine. «La sicurezza digitale passa anche dalla consapevolezza: riconoscere i segnali di una truffa è il primo passo per difendersi e proteggere sé stessi e gli altri», ricordano i militari dell'arma.