

Truffa della ballerina WhatsApp: un attacco che sfrutta la fiducia



La truffa della ballerina WhatsApp rappresenta l'ultima evoluzione di una categoria di attacchi che i professionisti della sicurezza osservano con crescente preoccupazione: lo *smishing* relazionale. Non parliamo di un semplice tentativo di *phishing* massivo, ma di un meccanismo sofisticato che trasforma ogni vittima in un vettore di propagazione, sfruttando il patrimonio più prezioso nelle comunicazioni digitali: la fiducia tra contatti conosciuti.

Il messaggio arriva da un amico, un familiare, un collega. Mostra l'immagine di una giovane ballerina in body nero e chiede un gesto apparentemente innocuo: votare per "Federica", presentata come la figlia di un'amica, affinché possa vincere una borsa di studio. Nessuna richiesta di denaro, nessun link palesemente sospetto. Eppure, in pochi secondi, l'intera identità digitale della vittima può passare nelle mani di cybercriminali.

Questo articolo offre un'analisi tecnica approfondita del fenomeno, esplorando i meccanismi psicologici che lo rendono efficace, le dinamiche di propagazione a catena e, soprattutto, le contromisure concrete che i professionisti della sicurezza possono implementare a livello individuale e organizzativo.

Il contesto: l'escalation delle truffe su WhatsApp in Italia

Prima di addentrarci nell'anatomia della truffa della

ballerina, è essenziale comprendere il contesto in cui si inserisce. I dati del Report annuale 2024 della Polizia Postale delineano uno scenario preoccupante: 18.714 casi di truffe online trattati, con un incremento del 15% rispetto all'anno precedente. Ma il dato più significativo riguarda le somme sottratte: 181 milioni di euro, in aumento del 32% rispetto ai 137 milioni del 2023.

Il Commissariato di P.S. Online ha registrato oltre 82.000 segnalazioni e 23.000 richieste di assistenza, con *smishing* e *spoofing* tra le tipologie più frequentemente riportate. Questi numeri fotografano un ecosistema criminale in rapida evoluzione, dove le tecniche di *social engineering* diventano sempre più raffinate e dove le piattaforme di messaggistica istantanea costituiscono il terreno di caccia privilegiato.

WhatsApp, con oltre 35 milioni di utenti attivi in Italia e un tasso di penetrazione che sfiora il 90% nella fascia 16-64 anni secondo il Digital Report 2024 di We Are Social, rappresenta un bersaglio ideale: la percezione di sicurezza garantita dalla crittografia *end-to-end*, combinata con la natura informale delle conversazioni, crea un ambiente dove le difese cognitive degli utenti risultano strutturalmente abbassate.

Come funziona la truffa della ballerina WhatsApp

Il pretesto emotivo

La truffa della ballerina si distingue per l'ingegneria sociale raffinata che ne costituisce il nucleo. Il messaggio tipo recita: *"Ciao! Per favore vota per Federica in questo sondaggio, è la figlia di una mia amica. Il premio principale è una borsa di studio per l'istruzione gratuita per tutto il prossimo anno, questo è molto importante per lei"*.

L'efficacia di questo pretesto risiede in diversi elementi psicologici accuratamente orchestrati:

- Appello all'empatia: aiutare una giovane a realizzare un sogno attraverso un gesto minimo;
- Assenza di richieste economiche dirette: nessun campanello d'allarme legato al denaro nella fase iniziale;
- Legittimazione sociale: il messaggio proviene da un contatto conosciuto, già presente in rubrica;
- Basso *effort* percepito: "basta un click", un'azione che non richiede impegno cognitivo.

L'immagine della ballerina in body nero durante un'evoluzione artistica completa il quadro, aggiungendo un elemento visivo che rafforza la credibilità del racconto.

Il meccanismo tecnico: *device linking hijacking*

Dal punto di vista tecnico, la truffa della ballerina sfrutta una vulnerabilità non nel software, ma nel design dell'esperienza utente di WhatsApp. Il link contenuto nel messaggio conduce a una pagina che imita l'aspetto di Facebook o di un portale di votazioni. Qui inizia la fase critica dell'attacco.

La pagina richiede alla vittima di inserire il proprio numero di telefono per "confermare il voto". In background, gli attaccanti utilizzano questo numero per avviare una richiesta di *device pairing* attraverso l'infrastruttura legittima di WhatsApp Web.

Il sistema genera un codice numerico a sei cifre che viene inviato via SMS alla vittima. La pagina fraudolenta presenta questo codice come "conferma della votazione", istruendo l'utente a inserirlo nell'app WhatsApp. La vittima, credendo di completare una procedura di verifica routinaria, sta in realtà autorizzando il collegamento di un dispositivo controllato dagli attaccanti al proprio account.

Questo approccio, che i ricercatori di Gen Digital hanno denominato *GhostPairing Attack* nella loro ricerca pubblicata il 15 dicembre 2025, rappresenta un'evoluzione significativa rispetto alle tecniche tradizionali di *account takeover*. Non richiede il furto di password, l'intercettazione di SMS, né il *SIM swapping*. Sfrutta esclusivamente le funzionalità legittime della piattaforma e l'inconsapevolezza dell'utente.

L'accesso persistente

Una volta completato il *pairing*, il browser dell'attaccante risulta collegato all'account della vittima con le stesse capacità di una sessione WhatsApp Web legittima:

- Lettura delle conversazioni storiche sincronizzate;
- Ricezione in tempo reale di tutti i nuovi messaggi;
- Visualizzazione e download di foto, video e note vocali;
- Invio di messaggi a singoli contatti e gruppi;
- Accesso a informazioni sensibili condivise nelle chat (indirizzi, credenziali, documenti).

L'aspetto più insidioso è che il telefono della vittima continua a funzionare normalmente. Non c'è alcun segnale evidente di compromissione. L'attaccante può rimanere connesso in background per giorni o settimane, monitorando silenziosamente ogni conversazione.

La propagazione virale: da vittima a vettore

Da vittima a vettore: la catena del contagio

La truffa della ballerina WhatsApp presenta caratteristiche che la rendono particolarmente virulenta sotto il profilo della propagazione. Ogni account compromesso diventa automaticamente un nuovo punto di distribuzione, con accesso immediato all'intera rubrica della vittima.

Gli attaccanti non devono compiere alcuna azione manuale: il messaggio esca viene inoltrato a tutti i contatti, moltiplicando esponenzialmente il numero di potenziali vittime. In termini epidemiologici, siamo di fronte a un R_0 (numero di riproduzione di base) potenzialmente molto elevato, dove ogni "infetto" può contagiare decine o centinaia di nuovi bersagli.

Il fattore critico è la fiducia preesistente. Quando riceviamo un messaggio da un contatto noto, il nostro sistema cognitivo tende a bypassare i normali filtri di valutazione critica. È un meccanismo evolutivo che, nel contesto digitale, si trasforma in una vulnerabilità sistemica.

La monetizzazione: dalle richieste di denaro all'estorsione

La compromissione dell'account rappresenta solo la prima fase dell'attacco. La monetizzazione avviene tipicamente attraverso due canali:

Richieste di prestito urgente: dai numeri compromessi partono messaggi ai contatti più stretti (familiari, amici intimi) che lamentano difficoltà economiche improvvise e richiedono bonifici immediati. La familiarità del mittente e l'urgenza del tono abbattano le resistenze.

Estorsione basata su contenuti sensibili: l'accesso prolungato alle conversazioni consente agli attaccanti di raccogliere informazioni compromettenti, foto private, dettagli personali che possono essere utilizzati per ricatti successivi.

La vittima primaria, nel frattempo, scopre la compromissione solo quando viene contattata da conoscenti insospettiti dalle strane richieste ricevute a suo nome.

Il substrato psicologico: perché funziona

I *bias* cognitivi sfruttati

La truffa della ballerina rappresenta un caso di studio esemplare di come il *social engineering* sfrutti i *bias* cognitivi fondamentali:

Bias di familiarità: tendiamo a fidarci di ciò che ci è familiare. Un messaggio da un contatto noto attiva automaticamente un *frame* mentale di sicurezza.

Principio di reciprocità: la richiesta di un “piccolo favore” attiva il desiderio di contraccambiare la relazione sociale, anche se il favore richiesto comporta rischi non percepiti.

Prova sociale implicita: se il nostro amico ci chiede di votare, significa che lui stesso ha valutato l’iniziativa come legittima. Deleghiamo inconsciamente a lui il processo di *due diligence*.

Urgenza e scarsità: la borsa di studio “importante”, il concorso con scadenza, creano una pressione temporale che riduce lo spazio per la riflessione critica.

Normalizzazione delle verifiche: nell’ecosistema digitale contemporaneo, inserire codici, confermare identità, autorizzare accessi sono azioni quotidiane. La richiesta non appare anomala perché si inserisce in un *pattern* comportamentale consolidato.

La neutralizzazione delle difese

Il design dell’attacco è calibrato per neutralizzare le difese cognitive tipiche:

- Nessuna richiesta di denaro iniziale → nessun allarme economico

- Nessun link a domini palesemente sospetti → nessun allarme tecnico
- Mittente conosciuto → nessun allarme relazionale
- Azione apparentemente banale → nessun allarme di proporzionalità

Quando tutti i semafori sono verdi, il sistema cognitivo procede in modalità automatica, senza attivare il pensiero critico che potrebbe intercettare la minaccia.

Implicazioni per la sicurezza aziendale

WhatsApp come shadow IT

Per i CISO e i *security architect*, la truffa della ballerina solleva questioni che trascendono la sfera personale. WhatsApp rappresenta una delle forme più pervasive di *shadow IT*: utilizzato massivamente per comunicazioni di lavoro, spesso veicola informazioni sensibili, documenti aziendali, credenziali condivise “al volo”.

Un account compromesso può esporre:

- Conversazioni con clienti e fornitori;
- Documenti confidenziali condivisi via chat;
- Credenziali e codici OTP scambiati informalmente;
- Informazioni su struttura organizzativa e processi interni.

L'attaccante che ottiene accesso persistente a un account aziendale acquisisce una posizione privilegiata per attacchi successivi di tipo BEC (*Business Email Compromise*) o per operazioni di spionaggio industriale.

Il vettore di compromissione interna

La propagazione virale della truffa implica che la compromissione di un singolo dipendente può rapidamente

estendersi a colleghi, superiori, partner commerciali. Il messaggio fraudolento che arriva dal telefono del CFO al team finance acquisisce una credibilità che nessuna email di *phishing* potrebbe mai raggiungere.

Contromisure e difese pratiche

Autodifesa digitale

Verifica *out-of-band*: prima di cliccare qualsiasi link che richieda azioni di conferma, contattare il mittente attraverso un canale alternativo (telefonata, SMS diretto, altro social) per verificare l'autenticità della richiesta.

Attivazione della verifica in due passaggi: nelle impostazioni di WhatsApp, la funzione aggiunge un PIN personale che gli attaccanti non possono impostare o modificare, riducendo l'impatto di alcune varianti dell'attacco.

Audit periodico dei dispositivi collegati: navigare regolarmente in Impostazioni → Dispositivi collegati e disconnettere qualsiasi sessione non riconosciuta. È l'unico modo per rilevare una compromissione silenziosa.

Consapevolezza del *pattern*: qualsiasi richiesta di inserire codici ricevuti via SMS in contesti diversi dal login diretto a un servizio deve essere trattata come potenzialmente malevola.

Per le organizzazioni

Policy di comunicazione: definire chiaramente quali canali sono autorizzati per la condivisione di informazioni sensibili, escludendo esplicitamente le app di messaggistica personale.

Awareness training specifico: integrare nei programmi di formazione sulla sicurezza scenari basati su *smishing* relazionale, simulando attacchi che sfruttano la fiducia tra

colleghi.

Procedure di verifica per richieste finanziarie: implementare protocolli che richiedano conferma verbale diretta per qualsiasi richiesta di trasferimento fondi, indipendentemente dal canale di provenienza.

Monitoraggio delle segnalazioni: creare un canale interno per la raccolta rapida di segnalazioni di messaggi sospetti, consentendo l'identificazione precoce di *pattern* di attacco.

Cosa fare se si è vittima della truffa della ballerina

Chi sospetta di aver compromesso il proprio account deve agire immediatamente:

1. **Disconnettere tutti i dispositivi:** Impostazioni → Dispositivi collegati → disconnettere ogni sessione attiva;
2. **Avvisare i contatti:** informare familiari, amici e colleghi che potrebbero ricevere messaggi fraudolenti dal proprio numero;
3. **Attivare la verifica in due passaggi:** se non già attiva, impostarla immediatamente per prevenire ulteriori compromissioni;
4. **Documentare l'accaduto:** conservare screenshot e informazioni utili per un'eventuale denuncia;
5. **Segnalare alle autorità:** presentare denuncia alla Polizia Postale attraverso il portale del Commissariato di P.S. Online.

Riflessioni conclusive

La truffa della ballerina WhatsApp ci ricorda una verità scomoda: le difese tecnologiche più sofisticate possono essere aggirate sfruttando l'anello più debole della catena, ovvero il fattore umano. La crittografia *end-to-end* protegge i

messaggi in transito, ma non può nulla contro un utente che autorizza volontariamente l'accesso al proprio account.

Per i professionisti della sicurezza, questo caso offre spunti di riflessione su diversi fronti. Sul piano del design delle piattaforme, emerge la necessità di ripensare i flussi di *device linking* con *warning* più espliciti e contestualizzati. Sul piano della formazione, si conferma l'insufficienza degli approcci basati esclusivamente su indicatori tecnici (URL sospetti, errori grammaticali) a fronte di attacchi che sfruttano la dimensione relazionale.

La truffa della ballerina non sarà l'ultima evoluzione dello *smishing* relazionale. Gli attaccanti continueranno a perfezionare i pretesti, a sfruttare nuove funzionalità delle piattaforme, a identificare i punti ciechi delle nostre difese cognitive. La risposta non può essere solo tecnologica: richiede un investimento costante nella costruzione di una cultura della sicurezza che integri consapevolezza, procedure e strumenti in un approccio olistico alla protezione dell'identità digitale.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/truffa-della-ballerina-whatsapp/>