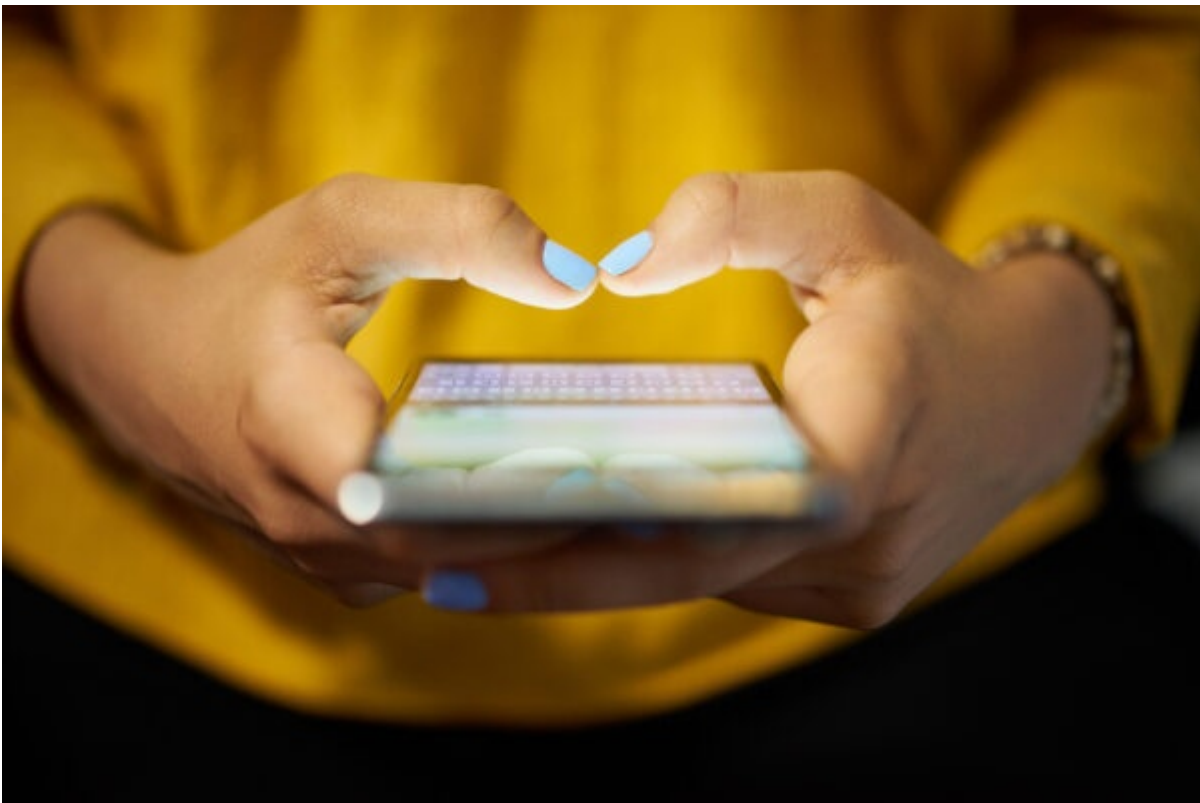




LA LEGGE PER TUTTI
INFORMAZIONE E CONSULENZA LEGALE

WhatsApp in versione rosa: cosa devi sapere

Autore: Denise Ubbriaco | 22/04/2021



Arriva un nuovo pericolo per gli utenti dell'app di messaggistica istantanea. Così gli utenti vengono truffati.

WhatsApp si è tinto di rosa? Assolutamente, no. La **versione Pink** che sta circolando sul web e che numerosi utenti hanno già scaricato, è una truffa.

Pertanto, attenzione a **non effettuare il download**.

WhatsApp Pink è l'ultima trovata dei **cyber-criminali** per intrufolarsi nei dispositivi degli utenti e sottrarre dati sensibili, contatti, messaggi, foto e, persino, le password del loro conto bancario.

Come riporta l'*Huffington Post*, è stato il ricercatore di sicurezza *Rajshekhar Rajaharia* a denunciare la **nuova truffa online** su Twitter e a mostrare, in un video, come funziona il *malware*.

In pratica, gli utenti ricevono un link che invita a scaricare questa "nuova" **versione di WhatsApp** in cui l'interfaccia cambierebbe colore passando dal classico verde al rosa. Una volta installata, l'applicazione svanisce improvvisamente dalla schermata principale del dispositivo e resta attiva in **background** rubando i dati delle vittime, prendendo il controllo della loro rubrica o inoltrando messaggi ai loro contatti con la richiesta di effettuazione del download dell'app. Ed è così che la truffa continua a diffondersi.

Come intervenire? Come mettere al sicuro il proprio dispositivo se è stato già effettuato il download? Bisogna **disinstallare** immediatamente **WhatsApp Pink** e chiudere tutte le sessioni attive dalla versione Web di WhatsApp accessibile dalle impostazioni dell'app ufficiale e cancellare la memoria del browser.

Ma la truffa della **versione rosa di WhatsApp** non è l'unica che sta spopolando in Rete nelle ultime ore. Circola anche la truffa del "**codice a 6 cifre**" che sfrutta appunto la sequenza di numeri necessaria per il trasferimento rapido dell'app di messaggistica istantanea nel momento in cui l'utente passa ad un altro smartphone oppure cambia il proprio numero di telefono.

Anche in questo caso, le vittime ricevono un **messaggio** da un contatto presente nella propria rubrica (già caduto nella trappola), in cui dichiara che è stato inoltrato il codice univoco tramite sms e, pertanto, richiede l'invio della sequenza numerica. Assecondando la richiesta e aprendo il **link ricevuto tramite sms**, si dà il via libera ai cyber-criminali che, anche stavolta, riusciranno ad accedere ai dati personali della vittima, alla sua **rubrica**, alle **carte di credito**. Una truffa che ha come conseguenze non solo il furto di identità, ma anche lo svuotamento del conto delle vittime ignare e l'effettuazione di spese non autorizzate.

Pertanto, per evitare di cadere in queste e in altre truffe online è sempre

consigliabile diffidare dai messaggi che invitano a cliccare su link o ad installare app sul proprio dispositivo.