



MESSAGGI TRUFFA DA RICONOSCERE

Gli inganni tramite sms e WhatsApp sono piuttosto diffusi. Tra la finta urgenza Tari, la “frode della ballerina” e i fantomatici uffici “Usi”, come funzionano questi raggiri e come difendersi.

di Luca Cartapatti





nostri smartphone aprono a un mondo di conoscenze e opportunità

impensabili solo fino a pochi anni fa. Allo stesso tempo, però, sono anche una porta d'accesso alle nostre informazioni, attraverso cui i criminali informatici riescono a raggiungerci sempre più facilmente. E le truffe via sms o WhatsApp sono ormai molto diffuse: ecco alcuni degli esempi più recenti, come riconoscere i tentativi di inganno e come tutelarsi.

IL FALSO SMS SULLA TARI

La truffa del messaggio sulla Tari (la tassa comunale sui rifiuti) è circolata negli ultimi mesi. Si tratta di un sms che segnala una posizione Tari irregolare e invita a chiamare un numero di telefono per comunicazioni urgenti. Si chiama smishing ed è una variante del phishing (via mail) che usa gli sms come esca. Il messaggio non arriva dal Comune o dal gestore della tassa sui rifiuti e il numero indicato è a tariffazione speciale (prefissi 893 o 895), per cui ogni minuto di conversazione può costare diversi euro. In più, durante la telefonata i truffatori possono cercare di ottenere informazioni sensibili come dati anagrafici, codice fiscale, coordinate bancarie, numeri di carta. Dati che vengono poi riutilizzati per altri scopi fraudolenti.

Il testo del messaggio è breve, ha un tono simile a quello ufficiale e richiama un tema delicato come quello dei tributi, proprio per questo motivo può risultare credibile; d'altro canto non fornisce dettagli, non cita dati personali e punta tutto sull'urgenza. Questo tipo di truffa funziona perché spinge a reagire subito, facendo leva sulla paura di avere

un problema fiscale. Il messaggio resta volutamente vago, non indica il nome del destinatario, non riporta una pratica e non cita con precisione l'ente che scrive. La cosa migliore da fare è semplice, cioè non chiamare il numero indicato, cancellare l'sms e segnalare il numero come spam tramite la funzione integrata dell'app messaggi dello smartphone. Se il messaggio mette

comunque in dubbio e si vuole essere certi di essere in regola con la propria posizione Tari, si possono utilizzare i canali ufficiali per verificare la propria posizione: il primo riferimento resta l'ufficio tributi del Comune o, dove previsto, il gestore del servizio Tari. Alcune amministrazioni inoltre permettono ai cittadini di consultare online la propria posizione fiscale tramite piattaforme digitali alle quali si



UN ESEMPIO DEL MESSAGGIO SULLA TASSA DEI RIFIUTI

Sms come questi, o simili, sono stati segnalati da varie regioni italiane. Sindaci e amministrazioni comunali si sono attivati per informare la popolazione. Anche SO.G.E.T. S.p.A., società che gestisce la riscossione dei tributi per conto di molti enti, ha confermato di non aver mai fatto l'invio.

Quali sono le differenze da riconoscere tra un messaggio truffaldino e le comunicazioni ufficiali sulla Tari.

	SMS TRUFFA	COMUNICAZIONI UFFICIALI
Dati personali	Nessuna identificazione personale	Viene riportato nome, cognome o codice fiscale
Dati dell'Ente	Generico, nessuna indicazione specifica	Nome del Comune, del gestore dei rifiuti e/o numero di pratica
Contatti	Numeri a tariffazione speciale con prefisso 893, 895, +39893, +39895	Rimando a siti istituzionali, del Comune o del gestore della Tari
Tono	Allarmistico/urgente senza riferimenti temporali	Tempistiche precise



CONCORSO DI DANZA CON INGANNO

Ecco il testo messaggio che pare arrivare da un contatto vero: "Ciao! Per favore votate per Federica in questo sondaggio, è la figlia di una mia amica, il premio principale è una borsa di studio per tutto il prossimo anno, questo è molto importante per lei. Grazie mille!"

può accedere con Spid, Cie o Cns. In alcuni casi le comunicazioni ufficiali possono comparire anche sull'app Io, se il Comune utilizza questo canale.

Se ormai siete stati vittime della truffa e quindi avete chiamato il numero indicato, ci sono due aspetti da controllare subito: il costo della chiamata e gli eventuali dati che potreste aver comunicato. Per quanto riguarda il primo punto, verificate con l'operatore se ci sono addebiti legati a numerazioni a sovrapprezzo e chiedete, se possibile, il blocco di questo tipo di servizi. Ma, soprattutto, se durante la telefonata avete fornito dati bancari o informazioni sulla carta, controllate i movimenti e valutate con la banca se bloccare gli strumenti di pagamento o cambiare le credenziali di accesso. Infine conservate il messaggio, fate uno screenshot e presentate una segnalazione alla Polizia Postale o alle forze dell'ordine.

UNA FINTA BIMBA BALLERINA

I tentativi di inganno possono raggiungerci anche tramite WhatsApp. Nel caso della cosiddetta "truffa della ballerina" il messaggio sembra arrivare da un contatto reale: un'amica, un collega, un parente. Il testo è semplice e punta tutto su una richiesta apparentemente innocua: votare una ragazza che partecipa a un concorso di danza. A volte il nome cambia, ma lo schema resta lo stesso: in una versione quasi identica, ad esempio, si parla di "votare la figlia della mia amica". Non c'è nessun virus visibile, nessun allegato sospetto e proprio per questo la truffa è ancora più

subdola, giocando totalmente sulle emozioni e l'empatia degli esseri umani e spingendo così l'utente a consegnare le chiavi del proprio account WhatsApp.

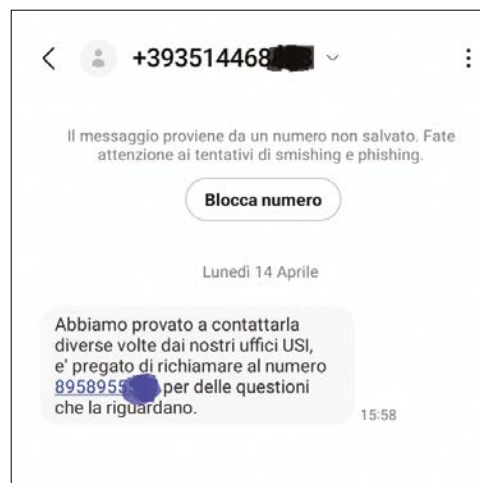
Nella pratica si riceve la foto di una ragazza, con un link esterno e l'invito a darle il proprio voto; la ragazza che bisogna votare sarebbe una ballerina che partecipa a un concorso di danza e che, proprio grazie al nostro voto, potrebbe vincere una borsa di studio. Cliccando sul link, si viene rimandati su un sito che a prima vista sembra credibile: grafica curata, foto, pulsanti per votare ben visibili. Ma per esprimere il proprio voto, viene chiesto di inserire il proprio numero di telefono e un codice che l'utente riceve via sms o WhatsApp.

La richiesta arriva in genere da un contatto di WhatsApp ed è emotivamente convincente; inoltre, spesso sottolinea che la possibilità di votare scade a breve. La combinazione di fiducia e urgenza riduce la soglia di attenzione. Il codice che viene chiesto, invece, non serve a votare, ma serve ai truffatori per collegare l'account WhatsApp dell'utente a un loro dispositivo tramite la funzione ufficiale di collegamento multi-dispositivo. In altre parole: stanno tentando un "pairing" a vostra insaputa, si tratta del cosiddetto "Ghost Pairing". Il pairing è una funzione legittima di WhatsApp che consente di usare l'account su più dispositivi (ad esempio su un computer tramite WhatsApp Web o Desktop). Per ➤➤

**NON CLICCARE SUI LINK E NON
RICHIAMARE I NUMERI INDICATI.
PUOI ANCHE SEGNALARE LA TRUFFA**

» attivarlo, basta inquadrare un QR code o inserire un codice di verifica. Il Ghost Pairing è l'uso fraudolento di questa funzione. Il truffatore avvia la procedura di collegamento dal proprio computer e induce a fornirgli il codice necessario per completarla. Se ci riesce, il suo dispositivo entra nell'elenco dei "Dispositivi collegati" dell'account dell'utente. Da quel momento può leggere conversazioni, inviare messaggi a suo nome ai suoi contatti (e quindi mandare avanti la truffa della ballerina), ma anche recuperare dati personali utili per altri raggiri, senza che l'utente se ne accorga. La buona notizia è che proteggersi è possibile:

- non inserite mai codici di verifica ricevuti via sms o WhatsApp su siti esterni, anche se sembrano legati a un concorso;
- attivate la verifica in due passaggi nelle impostazioni di WhatsApp (andando su "Account" e poi "Verifica in due passaggi");
- diffidate dei messaggi che chiedono voti, sostegno urgente o azioni rapide tramite link;
- se avete già cliccato e inserito un codice, il consiglio è quello di scollegare subito i dispositivi sospetti: toccate i tre puntini in alto a destra (oppure "Impostazioni" in basso a destra se avete un iPhone) e poi toccate la voce "Dispositivi collegati". Potreste notare i nomi di smartphone, pc o tablet che non riconoscete (ad esempio un dispositivo con Windows se sapete che usate solo Apple): toccate su ognuno dei dispositivi sospetti e rimuoveteli immediatamente con la funzione "Disconnetti / Esci", o se preferite cercate la voce "Disconnetti da tutti i dispositivi" e confermate l'operazione. Dopodiché attivate o modificate il pin della verifica in due passaggi: questo rende la vita più difficile ai



truffatori. Infine avvisate i vostri contatti che potrebbero ricevere messaggi anomali dal vostro numero, in modo che non caschino anche loro nel tranello.

I FANTOMATICI UFFICI "USI"

Un altro tipo di truffa che ad esempio è circolata qualche tempo fa è quella degli "uffici Usi" (vedi in alto). In questo caso prima arrivano telefonate da un numero sconosciuto; se non si risponde, arriva un sms in cui si chiede di richiamare lo stesso numero da cui si erano ricevute le chiamate: "Abbiamo provato a contattarla diverse volte dai nostri uffici Usi, è pregato di richiamare al numero 3514468XXX per delle questioni che la riguardano". Si tratta di un testo che mette un senso di urgenza e, visto che il numero indicato è lo stesso delle chiamate, insinua anche il dubbio rispetto al fatto che ci possa essere davvero qualcosa da chiarire all'"Usi" (uffici sanitari presenti solo in alcune regioni e che ovviamente hanno smentito). Il vero obiettivo di un messaggio così vago è far richiamare, perché poi da lì possono partire diverse altre

CHIAMANO E POI MANDANO ANCHE UN SMS

Con la truffa degli "uffici Usi" si ricevono telefonate e poi anche un messaggio: "Abbiamo provato a contattarla diverse volte dai nostri uffici USI, è pregato di richiamare al numero 3514468XXX per delle questioni che la riguardano".

"possibilità": tentativi di ottenere dati personali, pressioni per pagamenti non dovuti ecc.

UN AIUTO PER SEGNALARE

Queste truffe via sms o WhatsApp si inseriscono in un panorama più ampio di raggiri digitali, fatti anche di mail o telefonate con voci clonate. Per aiutare i consumatori a reagire, ma anche a informare e proteggere altri utenti tramite la loro esperienza, abbiamo creato una piattaforma per segnalare le truffe online nell'ambito del progetto Digitalizzati: altroconsumo.it/segnala-truffa ●

DIGITALIZZATI

Finanziato dal MIMIT. D.D. 12 maggio 2025

EDUCAZIONE DIGITALE E FRODI

Articolo realizzato nell'ambito di DIGITALIZZATI, il progetto con cui puntiamo a rafforzare le competenze digitali dei cittadini aiutandoli a difendersi dalle frodi online altroconsumo.it/digitalizzati