



Sos anziani per truffe telefoniche? Arriva l'app che risponde ai numeri sconosciuti

Descrizione

(Adnkronos) Ad agosto le città si svuotano, ma per milioni di anziani italiani la solitudine diventa la prima vulnerabilità da difendere. Anche dalle truffe telefoniche. Non è solo il fastidio del telemarketing selvaggio: dietro uno squillo da un numero sconosciuto si nascondono sempre più spesso organizzazioni criminali che sfruttano l'intelligenza artificiale per clonare voci familiari e tecniche di spoofing per far apparire sul display il numero reale della propria banca o delle forze dell'ordine. I dati confermano che non si tratta di un allarme episodico. Secondo il dossier di Consumerismo No Profit, nel triennio 2022-2024 le truffe telefoniche hanno sottratto ai cittadini italiani 559,4 milioni di euro, con 2,8 milioni di vittime stimate nel solo 2024 e una crescita del fenomeno del +30% nell'ultimo anno.

Un quadro che si aggrava ulteriormente quando si guarda alla popolazione anziana, oggi 14,8 milioni di persone pari a circa un quarto degli italiani: secondo il Rapporto Italia 2025 di Eurispes, elaborato sui dati del ministero dell'Interno, le vittime di truffa over 65 sono salite a 42.890 nel 2024, in aumento del 15,58% rispetto ai 37.108 casi del 2023. Le truffe telefoniche restano la tipologia più diffusa contro gli anziani, indicata dal 71% di chi ne denuncia conoscenza diretta o indiretta.

Nonostante l'attenzione, l'errore umano resta possibile, soprattutto davanti a tecnologie capaci di clonare perfettamente le voci. Per eliminare il rischio alla radice, Startup Service ha creato Devia, l'applicazione che ribalta il paradigma della sicurezza attraverso il filtro umano, particolarmente utile nei mesi estivi, quando i familiari stretti sono spesso irraggiungibili o lontani. Quando l'app è attiva, le telefonate da numeri non in rubrica vengono deviate a un centro servizi dove professionisti della sicurezza rispondono al posto dell'utente, identificano chi sta chiamando e ne verificano le reali intenzioni: solo se la chiamata è ritenuta sicura viene inoltrata in tempo reale allo smartphone dell'utente.

La tecnologia da sola non basta perché i truffatori hanno imparato a ingannare i software. Con Devia abbiamo scelto di rimettere l'uomo al centro: un operatore in carne ed ossa, l'unico in grado di riconoscere un tentativo di raggirio complesso, proteggendo non solo il portafoglio, ma anche la tranquillità quotidiana delle persone, specialmente d'estate, quando chi è più fragile

resta più esposto, spiega Giuseppe Dell'Acqua Brunone, Ceo di Stantup Service, che ha stilato anche cinque regole da seguire per la sicurezza telefonica.

1. La trappola del "Sì-à": l'importanza dei primi secondi. Mai esordire con un "Sì-à" quando si risponde a un numero sconosciuto. I truffatori utilizzano domande banali ("Mi sente?", "Sì? lei il signor...") per registrare il vostro assenso vocale, poi montato ad arte per simulare la stipula di contratti mai richiesti. Meglio un neutro "Pronto" o "Chi parla?".
2. La sacralità dei dati sensibili e dei codici Otp. Nessuna banca, ufficio postale o ente pubblico chiede mai telefonicamente codici Pin, password o codici Otp ricevuti via sms. Se chi chiama sostiene che il conto è "sotto attacco" e li richiede per "metterlo in sicurezza", è un tentativo di frode.
3. Il pressing psicologico e la falsa urgenza. La fretta è la migliore amica del truffatore: "Suo figlio ha avuto un incidente", "Il conto verrà bloccato tra 10 minuti". In estate, con i familiari lontani per le vacanze, questa leva è ancora più efficace sugli anziani soli. Quando l'interlocutore impedisce di riflettere o di consultarsi con un familiare, bisogna riagganciare subito.
4. Verifica attiva contro lo spoofing. I criminali possono manipolare il display facendo apparire numeri reali, come quello della banca o delle forze dell'ordine. Se la chiamata è sospetta: chiudere, cercare il numero ufficiale su un documento cartaceo o sul sito dell'ente, digitare i numeri manualmente per richiamare.
5. Il pericolo dei link nei "messaggi civetta". Spesso, durante o subito dopo la telefonata, arriva un sms con un link da cliccare per "annullare l'operazione sospetta". Portano a siti clone pensati per rubare le credenziali. Le banche non inviano mai link esterni via sms per le notifiche.

??

cronaca

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Agosto 8, 2026

Autore

redazione