

Iliad e la denuncia per la truffa dello «spoofing»: come funzionano le telefonate camuffate che valgono da contratto

Le truffe telefoniche manipolano i numeri di chiamata per ingannare le vittime. Spinti dall'urgenza, gli utenti forniscono dati personali e sottoscrivono nuovi contratti. Dopo i tentativi di truffa ai suoi stessi dipendenti, Iliad ha fatto un esposto al Tribunale di Milano (Fonte: <https://www.corriere.it/> 4 giugno 2025)



Il telefono squilla. Sul display appare un numero cellulare italiano, non memorizzato. Sconosciuto. Sarà il solito operatore che propone una nuova offerta per le bollette, pensa **Michele Rillo**, 34enne di Benevento, residente a Roma. Quando risponde, dall'altra parte scatta una voce registrata: «Gentile cliente, a breve avverrà una rimodulazione contrattuale». E poi l'invito a premere un tasto per selezionare l'operatore con cui hai sottoscritto il contratto. Il meccanismo è sostanzialmente «a tappeto»: vengono citati tutti i principali operatori telefonici. In questo caso, Michele è un utente Iliad e, dunque, seleziona il tasto 9 corrispondente. A questo punto, viene trasferito finalmente a un operatore di call center in carne e ossa.

La signorina che risponde, spacciandosi per dipendente Iliad, conferma un imminente «disservizio sulla linea» e una conseguente «rimodulazione tariffaria», spingendo Michele a migrare quanto prima verso un nuovo contratto, per evitare di soffrire i disservizi. Ed è in questo momento che entra in gioco un'altra operatrice del call center, stavolta in rappresentanza di un fantomatico - e inesistente - «servizio ministeriale di tutela del consumatore». L'operatrice verifica la miglior offerta al momento attiva e chiede a Michele la disponibilità a essere ricontattato; lui accetta, e di lì a poco viene effettivamente contattato da un altro operatore di call center, per conto di una

compagnia telefonica. Ma ciò che gli operatori-truffatori non sanno è che stavolta hanno composto il numero sbagliato: **Michele Rillo, infatti, oltre a essere un cliente Iliad, è anche dipendente della stessa compagnia telefonica** e, da tempo, l'azienda è impegnata nel contrasto a questi comportamenti ingannevoli. Con la registrazione della chiamata truffaldina ([vedi qui il video](#)), Michele Rillo - insieme ad un'altra collega e all'azienda stessa - ha presentato un esposto al Tribunale di Milano.

La tecnica del Cli Spoofing

Dietro la storia di Michele Rillo, simile a migliaia di storie identiche che ogni giorno vengono preannunciate dallo squillo di una telefonata automatica, si nasconde un sofisticato espediente: il **Cli Spoofing** (acronimo di Calling Line Identification Spoofing), una tecnica che permette di far comparire sul dispositivo del destinatario un numero di telefono diverso da quello reale. Il numero che appare sullo schermo è stato dunque manipolato, mascherando la vera identità del chiamante e facendolo sembrare una comunicazione ufficiale da parte di un'azienda o un servizio a cui ci si è affidati. La trappola è tesa e quando l'utente ignaro risponde, **un fiume di informazioni personali viene carpito attraverso un inganno** che si basa sulla stessa fiducia di chi ha risposto malauguratamente alla chiamata.

Il meccanismo della frode

Ma come funziona esattamente il meccanismo di questa frode? Proviamo a spiegarlo passo per passo.

1) Cli Spoofing. La prima cosa che fa il truffatore è quella di manomettere il Calling Line Identification (Cli) per effettuare la telefonata. Come detto, l'espedito tecnico consente di mascherare il calling ID autentico e far quindi apparire sul display dello smartphone del destinatario un numero credibile, quando invece la chiamata parte da un centralino (italiano o estero).

2) Agenzia di «lead generation». La chiamata è incentrata su una urgenza (caratterizzata da una narrativa costruita sulla base di informazioni false), che serve a carpire la fiducia dell'utente. Quest'ultimo, persuaso dalla situazione di emergenza, fornisce i dati di contatto («lead»), che verranno poi rivenduti a terzi come potenziali clienti.

3) Canale di teleselling. Dopo l'avvenuto contatto, generato come detto con modalità ingannevole, il malcapitato approda a un altro call center che, stavolta in modo formalmente regolare, sottopone un'offerta e attiva il contratto per conto di un terzo operatore.

Perché l'esposto di Iliad

Recentemente, l'**Autorità Garante delle Comunicazioni** è intervenuta con un provvedimento di **contrasto proprio al Cli Spoofing** e anche [l'Antitrust poche settimane fa ha avviato un](#)

[procedimento specifico per telemarketing scorretto](#). L'idea di Iliad, alla base della decisione di presentare un esposto, è che lo Spoofing sia sì il mezzo attraverso cui vengono perpetrare queste truffe, ma che il problema debba essere estirpato alla radice e, cioè, individuando e perseguendo la filiera criminale che monetizza lead ottenuti con menzogne, una vera e propria truffa. Per questo l'azienda ha depositato l'esposto alla Procura e segnalato il caso ad Agcom per chiedere di colpire il business model fin dalla sua origine, ovvero «chi fabbrica contatti usando informazioni false che ledono l'immagine delle aziende menzionate e conseguentemente sia la trasparenza che la fiducia nel mercato», come spiega l'ad di Iliad **Benedetto Levi** a Corriere.it.

«Frodi di questo tipo sono ormai di massa», prosegue Levi. «È nostra convinzione che **queste attività danneggino la reputazione e la fiducia di intere filiere industriali**, oltre a svilire completamente il canale delle vendite telefoniche. Il nostro esposto», conclude l'amministratore delegato di Iliad, «punta proprio a colpire la causa del fenomeno, e cioè le dichiarazioni false e truffaldine tramite le quali queste società acquisiscono, trattano e cedono i dati personali degli utenti».

Leggi anche

[Telemarketing, boom di truffe telefoniche: Antitrust avvia istruttoria su 7 call center \(e parte una petizione per dire basta\)](#)