Telefonate o messaggi truffa, basta rispondere per essere incastrati? Quali sono i rischi, e cosa fare

La quantità e la tipologia di raggiri che cercano di pescarci dal telefono si sono moltiplicati. In attesa di una soluzione tecnologica da parte di Agcom, conoscere le modalità e i comportamenti corretti è la forma di difesa migliore

(Fonte: https://www.corriere.it/tecnologia/ 21 aprile 2025)

Una delle scocciature che affliggono da anni gli italiani - con un grande aumento in questo ultimo periodo - è senz'altro quella delle telefonate o i messaggi truffaldini che mietono vittime grazie alla tecnica chiamata «spoofing». **Non è una tecnica nuova che consente ai malintenzionati di camuffare il numero reale del call center da cui parte la telefonata** (in genere attraverso un software VoIP - *voice over ip*) con un numero apparentemente attendibile. Che può essere un numero casuale oppure un numero di istituti bancari e simili. Nel tentativo di limitare queste chiamate è stato potenziato negli anni scorsi il **Registro delle Opposizioni** ai quali vi si sono iscritti milioni di utenti ma senza troppo successo. Anche il **codice di condotta per le agenzie** di telemarketing non può fare molto. Questo perché i call center da cui partono chiamate e sms non sono italiani, ma perlopiù esteri. Ma non è raro che i tentati raggiri partano anche dall'Italia. **Ora al vaglio c'è una soluzione** studiata da **Agcom** e dal **ministro delle Imprese e del Made in Italy**.

Come comportarsi e i rischi

Viene naturale chiedersi quali siano i rischi quando si risponde alle telefonate. La risposta è: **dipende**. Non c'è alcun rischio a rispondere alle telefonate, almeno finché non si consegnano dati sensibili, **o quando si clicca sui link** contenuti nei messaggi. In questo caso invece vi è la possibilità di **infettare il proprio dispositivo con virus o malware** difficili da rilevare e consegnare i propri dati di accesso o di pagamento. Esistono dei casi in cui si può essere danneggiati con una telefonata, ma in genere succede **quando è l'utente a effettuare una chiamata in uscita.** Dunque, specie nel caso di telefonate senza risposta da numeri esteri, **è meglio non richiamare**. Ma quali sono i vari casi in cui viene utilizzata la tecnica dello *spoofing* (o simili) e i rischi correlati?

Le chiamate con numeri inesistenti

Questo tipo di telefonate arrivano da numeri altrimenti attendibili e con numeri di telefono di operatori mobili con prefisso italiano. I filtri di Google come l'app come *TrueCaller* sono in grado, spesso, di identificare questi numeri come **spam**, ma sono creati in modo casuale. Alle volte possono essere inesistenti. A chiunque sarà capitato, almeno una volta, di ricevere una telefonata da un numero sconosciuto e una volta richiamato sentire la voce registrata del nostro operatore dire che **il numero è inesistente**. In questo caso non ci sono particolari pericoli. Tuttalpiù, quando si risponde a queste telefonate, si sentirà una voce registrata che inviterà l'utente ad investire nel

Forex, in criptovalute o in falsi investimenti in cui vengono coinvolti loro malgrado entità come Amazon, a cui ovviamente questi call center non sono in alcun modo correlati.

Le telefonate con un numero simile

Questa è una delle tattiche più subdole e viene utilizzata quando si ha un particolare obiettivo. Viene utilizzata infatti, come spesso accade nelle truffe, l'**ingegneria sociale**. In questa elaborato raggiro, si cerca di ottenere la fiducia della potenziale vittima, in primo luogo suscitandole curiosità. La telefonata che si riceve proviene infatti da un numero simile al proprio. Un espediente con cui si cerca di «agganciare» il proprio obiettivo e da lì instaurare un rapporto di fiducia. Nel mirino? Informazioni sensibili e strategiche. Bisogna sempre mantenere una sana dose di scetticismo e ricordarsi, come regola generale, che nessuno regala nulla.

Gli Sms (smishing)

Questi Sms sono tra i più pericolosi. I malfattori riescono a replicare perfettamente il numero autentico di banche e altri enti di credito o corrieri. Con una scusa più o meno credibile, invitano l'utente a raggiungere un indirizzo Web facendo cliccare loro un testo in cui vengono emulati i loghi e l'interfaccia grafica del sito originale. Il più delle volte vengono richiesti, come abbiamo raccontato qui, i dati delle carte di credito, in modo da poterle utilizzare per ritirare denaro o fare acquisti ingenti a proprie spese. Da tenere sempre a mente che gli istituti bancari, corrieri e poste, **non utilizzano mai gli Sms o le telefonate** per ottenere dati sensibili di ogni tipo.

Le telefonate mute

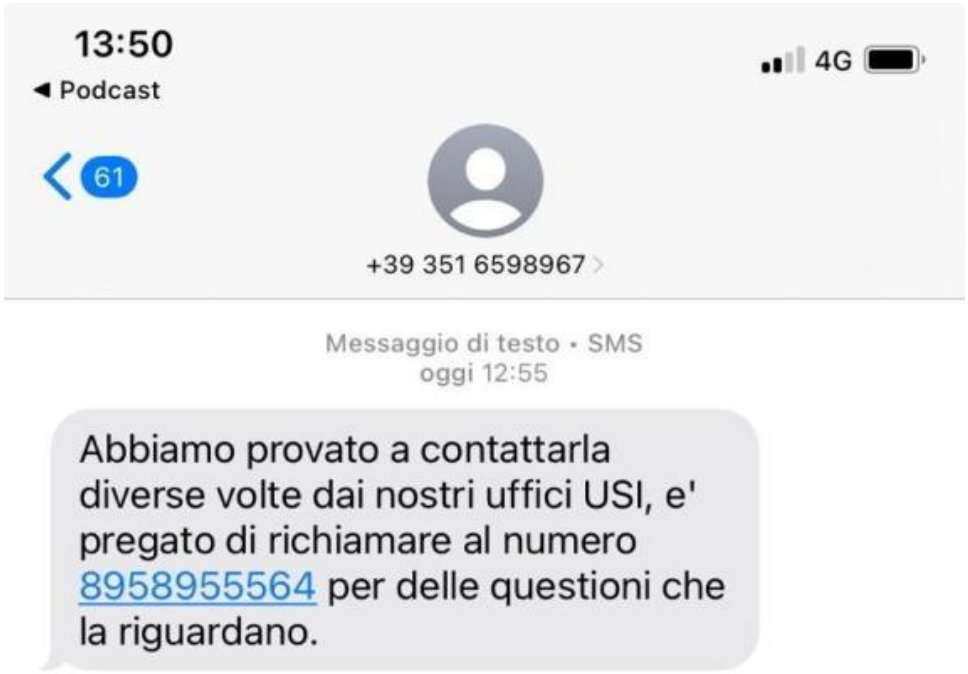
Un ampio approfondimento relativo a questa pratica lo offre il Garante della Privacy. In questo caso, nemmeno raro, le telefonate alle quali si risponde, sono caratterizzate da brusio di sottofondo, oppure nessun suono. Le telefonate mute avvengono quando il software utilizzato dal call center **genera più chiamate di quante gli operatori riescono a gestire**. Si tratta dunque di un sistema automatizzato e il silenzio è in genere interrotto quando il primo operatore disponibile si libera dalla telefonata precedente.

Oltre al rischio di cadere in un inganno, **c'è anche un aspetto psicologico da considerare**. Le chiamate mute infatti possono suscitare ansia nell'utente, che può temere di essere vittima di un altro genere di illecito, come stalking, intrusioni da malintenzionati di qualsiasi natura... Ecco perché viene utilizzato il brusio di sottofondo, chiamato anche «comfort noise». Il brusio consente di tranquillizzare l'utente sul fatto che la chiamata arrivi da un ufficio o comunque un contesto lavorativo.

La truffa del curriculum

Una delle ultime telefonate truffaldine riguardano le chiamate ricevute da false agenzie che ci informano di aver ricevuto il proprio curriculum. Si tratta di una modalità diversa di «ingaggiare» le vittime, in particolare chi è davvero in cerca di lavoro o necessita di un guadagno extra. Inizialmente, questi malintenzionati, contattavano le vittime tramite WhatsApp, dove venivano convinti a lasciare like a video per ottenere un pagamento che inizialmente arrivava davvero e di modica entità. Una volta ottenuta la fiducia della vittima e ingolosito dai pagamenti (in realtà eseguiti da altre vittime) vengono poi convinte ad entrare all'interno di un raggiro in cui eseguono pagamenti che hanno come scopo il riciclo di denaro.

Questa truffa, chiamata la truffa del mulo (*money muling*), porta numerosi rischi alle vittime. Non è solo la perdita di denaro a colpire, ma anche la spontanea partecipazione ad uno spostamento di denaro di natura criminale. **La partecipazione a questo meccanismo può essere consapevole o inconsapevole**, ma i rischi sono i medesimi. In un approfondimento, abbiamo raccontato le origini di questa truffa, che parte da centri disseminati nel sud est asiatico in cui veri eserciti di truffatori sono costretti e addestrati per ottenere più soldi possibili dalle vittime.



Il wangiri, la truffa dello squillo

La truffa del wangiri è una delle più subdole, perché è quella che sottrae nell'immediato denaro all'utente senza particolari stratagemmi. In genere, si riceve una chiamata, o meglio, uno squillo da un numero estero. Lo squillo è fatto in modo che l'utente non abbia il tempo necessario a rispondere, motivo per cui richiama il numero della telefonata senza risposta. Quando si richiama, viene però sottratto del credito. Alle volte i costi vengono addebitati e associati a servizi telefonici tutt'altro che gratuiti **oppure vengono attivati abbonamenti a servizi premium dal costo elevato**.

Come tutelarsi?

Le tentate truffe sono molte, ma sono diversi i modi in cui ci si può difendere. Il primo è mantenere **un sano scetticismo** verso le comunicazioni, apparentemente legittime. Bisogna inoltre ricordare che istituti bancari e servizi come corrieri o poste, non chiedono credenziali per e-mail o telefonate. E mai richiamare numeri sconosciuti o cliccare sui link negli sms o in generale nei messaggi.