Truffe con voce clonata dall'AI: come verificare una chiamata prima di fidarsi

Maria Cattini | 04/07/2026 | Sicurezza digitale

Il telefono squilla.

Sul display compare un numero familiare, o almeno plausibile. Dall'altra parte c'è una voce agitata: un figlio, un nipote, un collega, un amico. Dice che è successo qualcosa, che serve aiuto subito, che non c'è tempo per pensarci.

Il problema è che oggi la voce non basta più.

Una truffa telefonica può usare un numero falsificato, una storia urgente e una voce generata o modificata con l'intelligenza artificiale. Non serve immaginare scenari da film: il punto è molto più concreto. Se una persona pubblica audio, video, note vocali, interviste, reel o storie online, quella voce può diventare materiale da imitare.

La domanda pratica non è "riesco a capire se è AI?".

La domanda utile è: **come verifico la chiamata senza fidarmi della voce?**

Che cosa sono le truffe con voce clonata

Una truffa con voce clonata usa sistemi di sintesi vocale o manipolazione audio per imitare una persona reale.

Può essere un familiare.

Può essere un capo.

Può essere un collega.

Può essere una figura pubblica usata in un falso investimento, in una falsa emergenza o in un messaggio costruito per sembrare credibile.

Il meccanismo non è nuovo nella logica: le truffe telefoniche esistono da anni. La parte nuova è la qualità dell'imitazione. La voce sintetica può rendere più credibile una storia che prima avrebbe avuto segnali più facili da riconoscere: tono strano, accento poco naturale, frasi generiche, esitazioni fuori posto.

L'FBI, nel suo Internet Crime Report 2025, segnala oltre 22 mila reclami collegati all'uso dell'intelligenza artificiale nel cybercrime, con perdite dichiarate superiori a 893 milioni di dollari. Nel rapporto vengono citati anche casi di voice cloning usati in truffe di tipo "distress", cioè emergenze familiari o personali costruite per spingere la vittima a inviare denaro.

Il punto non è che ogni telefonata sospetta usi l'AI.

Il punto è che la voce non può più essere trattata come prova di identità.

Perché non basta riconoscere la voce

Molte persone pensano: “Se fosse mio figlio, mia madre, il mio capo, lo riconoscerei”.

È un’idea comprensibile, ma fragile.

Quando una chiamata arriva in un momento di paura, fretta o pressione, il cervello cerca una spiegazione rapida. Se la voce assomiglia a quella giusta e la storia contiene dettagli plausibili, il rischio è completare da soli i pezzi mancanti.

La FTC, l’autorità statunitense per la tutela dei consumatori, lo spiega con un esempio molto semplice: una voce in panico dice di essere un nipote in difficoltà, chiede soldi e sembra davvero lui. Ma il consiglio operativo è netto: non fidarsi della voce, richiamare la persona usando un numero già conosciuto o verificare attraverso un altro familiare.

È qui che cambia il metodo.

Non devi dimostrare che la voce sia falsa.

Devi verificare che la richiesta sia vera.

Sono due cose diverse.

I segnali da trattare con cautela

Una chiamata sospetta non sempre sembra sospetta.

Proprio per questo conviene osservare la richiesta, non solo il tono della voce.

Fai attenzione se la persona:

• chiede soldi con urgenza;
• chiede bonifici, ricariche, criptovalute, gift card o codici;
• dice di non avvisare nessuno;
• chiede di restare al telefono mentre paghi;
• usa paura, vergogna o senso di colpa;
• sostiene che il numero non può essere richiamato;
• invia subito dopo un link o un documento;
• ti chiede dati personali, codici OTP o password;
• dice che “non c’è tempo” per verificare.

L’urgenza è una tecnica, non una prova.

Un familiare in difficoltà può essere agitato. Ma una richiesta urgente di denaro o dati va verificata comunque.

Il metodo dei tre canali

Per proteggerti, usa un metodo semplice: **non verificare mai la richiesta nello stesso canale in cui è arrivata**.

Se la richiesta arriva per telefono, non restare dentro quella chiamata.

Fai così:

1. Interrompi la chiamataNon devi discutere, convincere o smascherare nessuno. Chiudi.
2. Richiama un numero che conosci giàNon usare il numero appena comparso sul display se non sei sicuro. Usa il contatto salvato, un numero precedente, una rubrica affidabile o un canale già verificato.
3. Controlla con una seconda personaSe riguarda un familiare, chiama un altro familiare. Se riguarda il lavoro, contatta un collega o il responsabile tramite un canale ufficiale.

Questo metodo funziona perché rompe la pressione della truffa.

Il truffatore vuole tenerti dentro la sua storia. Tu devi uscire dalla storia e controllarla da fuori.

Una parola in famiglia può aiutare, ma non basta

Molti consigliano una parola segreta di famiglia.

Può essere utile, soprattutto con bambini, anziani o persone esposte a truffe telefoniche. Ma va usata bene.

Una buona parola di verifica deve essere:

• non pubblica;
• non legata a informazioni presenti sui social;
• facile da ricordare;
• cambiata se viene detta a persone esterne;
• usata solo per verificare, non come gioco da condividere.

Meglio evitare domande come:

• “come si chiama tua madre?”;
• “dove siamo stati in vacanza?”;
• “qual è il nome del cane?”.

Molte di queste informazioni possono essere trovate online, nei profili social, in vecchi post, in database violati o semplicemente indovinate.

Una parola concordata prima è più utile di una domanda basata su informazioni personali.

Ma non deve diventare l’unico controllo.

Se la richiesta riguarda denaro, dati o accessi, serve comunque una verifica indipendente.

Cosa fare se la chiamata sembra arrivare da un contatto vero

Un numero sul display non è una garanzia.

I truffatori possono usare tecniche di spoofing, cioè far apparire un numero diverso da quello reale. Per chi riceve, la chiamata può sembrare provenire da una banca, da un ente, da un ufficio o persino da un contatto conosciuto.

Per questo alcuni sistemi stanno introducendo funzioni di verifica delle chiamate. A giugno 2026, per esempio, Google ha annunciato una funzione in Phone by Google che segnala possibili chiamate in cui qualcuno finge di usare il numero di un contatto. È un segnale utile, ma non risolve tutto: funziona solo in condizioni specifiche, con dispositivi e app compatibili.

La regola resta la stessa.

Il telefono può aiutare a segnalare un rischio, ma non può sostituire il tuo metodo di verifica.

Se una chiamata chiede soldi, codici, password o azioni urgenti, non basta che arrivi dal numero giusto.

Cosa non fare

Ci sono alcune reazioni che aumentano il rischio.

Non restare al telefono per “capire meglio”.

Non inviare piccoli importi “per sicurezza”.

Non leggere codici OTP.

Non cliccare link ricevuti subito dopo la chiamata.

Non installare app di assistenza remota.

Non condividere documenti, foto della carta d’identità, coordinate bancarie o schermate.

Non richiamare numeri inviati dalla persona che sta facendo pressione.

Non fidarti di una videochiamata solo perché vedi un volto: anche immagini e video possono essere manipolati, registrati o usati fuori contesto.

Il controllo migliore è sempre esterno alla richiesta.

Checklist rapida

Quando ricevi una chiamata urgente, usa questa sequenza:

1. Fermati.
2. Non pagare durante la chiamata.
3. Non leggere codici.
4. Chiudi.
5. Richiama un numero già noto.
6. Verifica con un secondo contatto.
7. Se riguarda banca, lavoro o ente pubblico, usa solo canali ufficiali.
8. Conserva numero, orario, messaggi, screenshot e dettagli.
9. Segnala la truffa alla piattaforma, alla banca o alle autorità competenti.
10. Avvisa familiari e colleghi se la tua voce o il tuo nome potrebbero essere stati usati.

Non devi riconoscere l’AI.

Devi rallentare la richiesta.

La regola più importante

Una voce familiare può essere vera.

Può anche essere imitata.

Per questo la sicurezza non deve dipendere dall’orecchio, ma dal processo.

Se una persona cara ha davvero bisogno, sopporterà un minuto di verifica. Se un collega ti sta chiedendo un’azione urgente e legittima, potrà confermarla su un canale ufficiale. Se una banca o un

ente ti contatta davvero, non ti chiederà password, codici o pagamenti improvvisi dentro una telefonata emotiva.

La voce può convincere.

Il metodo deve controllare.
Il telefono squilla.

Sul display compare un numero familiare, o almeno plausibile. Dall'altra parte c'è una voce agitata: un figlio, un nipote, un collega, un amico. Dice che è successo qualcosa, che serve aiuto subito, che non c'è tempo per pensarci.

Il problema è che oggi la voce non basta più.

Una truffa telefonica può usare un numero falsificato, una storia urgente e una voce generata o modificata con l'intelligenza artificiale. Non serve immaginare scenari da film: il punto è molto più concreto. Se una persona pubblica audio, video, note vocali, interviste, reel o storie online, quella voce può diventare materiale da imitare.

La domanda pratica non è "riesco a capire se è AI?".

La domanda utile è: **come verifico la chiamata senza fidarmi della voce?**

Che cosa sono le truffe con voce clonata

Una truffa con voce clonata usa sistemi di sintesi vocale o manipolazione audio per imitare una persona reale.

Può essere un familiare.

Può essere un capo.

Può essere un collega.

Può essere una figura pubblica usata in un falso investimento, in una falsa emergenza o in un messaggio costruito per sembrare credibile.

Il meccanismo non è nuovo nella logica: le truffe telefoniche esistono da anni. La parte nuova è la qualità dell'imitazione. La voce sintetica può rendere più credibile una storia che prima avrebbe avuto segnali più facili da riconoscere: tono strano, accento poco naturale, frasi generiche, esitazioni fuori posto.

L'FBI, nel suo Internet Crime Report 2025, segnala oltre 22 mila reclami collegati all'uso dell'intelligenza artificiale nel cybercrime, con perdite dichiarate superiori a 893 milioni di dollari. Nel rapporto vengono citati anche casi di voice cloning usati in truffe di tipo "distress", cioè emergenze familiari o personali costruite per spingere la vittima a inviare denaro.

Il punto non è che ogni telefonata sospetta usi l'AI.

Il punto è che la voce non può più essere trattata come prova di identità.

Perché non basta riconoscere la voce

Molte persone pensano: "Se fosse mio figlio, mia madre, il mio capo, lo riconoscerei".

È un'idea comprensibile, ma fragile.

Quando una chiamata arriva in un momento di paura, fretta o pressione, il cervello cerca una spiegazione rapida. Se la voce assomiglia a quella giusta e la storia contiene dettagli plausibili, il

rischio è completare da soli i pezzi mancanti.

La FTC, l’autorità statunitense per la tutela dei consumatori, lo spiega con un esempio molto semplice: una voce in panico dice di essere un nipote in difficoltà, chiede soldi e sembra davvero lui. Ma il consiglio operativo è netto: non fidarsi della voce, richiamare la persona usando un numero già conosciuto o verificare attraverso un altro familiare.

È qui che cambia il metodo.

Non devi dimostrare che la voce sia falsa.

Devi verificare che la richiesta sia vera.

Sono due cose diverse.

I segnali da trattare con cautela

Una chiamata sospetta non sempre sembra sospetta.

Proprio per questo conviene osservare la richiesta, non solo il tono della voce.

Fai attenzione se la persona:

• chiede soldi con urgenza;
• chiede bonifici, ricariche, criptovalute, gift card o codici;
• dice di non avvisare nessuno;
• chiede di restare al telefono mentre paghi;
• usa paura, vergogna o senso di colpa;
• sostiene che il numero non può essere richiamato;
• invia subito dopo un link o un documento;
• ti chiede dati personali, codici OTP o password;
• dice che “non c’è tempo” per verificare.

L’urgenza è una tecnica, non una prova.

Un familiare in difficoltà può essere agitato. Ma una richiesta urgente di denaro o dati va verificata comunque.

Il metodo dei tre canali

Per proteggerti, usa un metodo semplice: **non verificare mai la richiesta nello stesso canale in cui è arrivata**.

Se la richiesta arriva per telefono, non restare dentro quella chiamata.

Fai così:

1. Interrompi la chiamataNon devi discutere, convincere o smascherare nessuno. Chiudi.
2. Richiama un numero che conosci giàNon usare il numero appena comparso sul display se non sei sicuro. Usa il contatto salvato, un numero precedente, una rubrica affidabile o un canale già verificato.
3. Controlla con una seconda personaSe riguarda un familiare, chiama un altro familiare. Se riguarda il lavoro, contatta un collega o il responsabile tramite un canale ufficiale.

Questo metodo funziona perché rompe la pressione della truffa.

Il truffatore vuole tenerti dentro la sua storia. Tu devi uscire dalla storia e controllarla da fuori.

Una parola in famiglia può aiutare, ma non basta

Molti consigliano una parola segreta di famiglia.

Può essere utile, soprattutto con bambini, anziani o persone esposte a truffe telefoniche. Ma va usata bene.

Una buona parola di verifica deve essere:

• non pubblica;
• non legata a informazioni presenti sui social;
• facile da ricordare;
• cambiata se viene detta a persone esterne;
• usata solo per verificare, non come gioco da condividere.

Meglio evitare domande come:

• “come si chiama tua madre?”;
• “dove siamo stati in vacanza?”;
• “qual è il nome del cane?”.

Molte di queste informazioni possono essere trovate online, nei profili social, in vecchi post, in database violati o semplicemente indovinate.

Una parola concordata prima è più utile di una domanda basata su informazioni personali.

Ma non deve diventare l’unico controllo.

Se la richiesta riguarda denaro, dati o accessi, serve comunque una verifica indipendente.

Cosa fare se la chiamata sembra arrivare da un contatto vero

Un numero sul display non è una garanzia.

I truffatori possono usare tecniche di spoofing, cioè far apparire un numero diverso da quello reale. Per chi riceve, la chiamata può sembrare provenire da una banca, da un ente, da un ufficio o persino da un contatto conosciuto.

Per questo alcuni sistemi stanno introducendo funzioni di verifica delle chiamate. A giugno 2026, per esempio, Google ha annunciato una funzione in Phone by Google che segnala possibili chiamate in cui qualcuno finge di usare il numero di un contatto. È un segnale utile, ma non risolve tutto: funziona solo in condizioni specifiche, con dispositivi e app compatibili.

La regola resta la stessa.

Il telefono può aiutare a segnalare un rischio, ma non può sostituire il tuo metodo di verifica.

Se una chiamata chiede soldi, codici, password o azioni urgenti, non basta che arrivi dal numero giusto.

Cosa non fare

Ci sono alcune reazioni che aumentano il rischio.

Non restare al telefono per “capire meglio”.

Non inviare piccoli importi “per sicurezza”.

Non leggere codici OTP.

Non cliccare link ricevuti subito dopo la chiamata.

Non installare app di assistenza remota.

Non condividere documenti, foto della carta d’identità, coordinate bancarie o schermate.

Non richiamare numeri inviati dalla persona che sta facendo pressione.

Non fidarti di una videochiamata solo perché vedi un volto: anche immagini e video possono essere manipolati, registrati o usati fuori contesto.

Il controllo migliore è sempre esterno alla richiesta.

Checklist rapida

Quando ricevi una chiamata urgente, usa questa sequenza:

1. Fermati.
2. Non pagare durante la chiamata.
3. Non leggere codici.
4. Chiudi.
5. Richiama un numero già noto.
6. Verifica con un secondo contatto.
7. Se riguarda banca, lavoro o ente pubblico, usa solo canali ufficiali.
8. Conserva numero, orario, messaggi, screenshot e dettagli.
9. Segnala la truffa alla piattaforma, alla banca o alle autorità competenti.
10. Avvisa familiari e colleghi se la tua voce o il tuo nome potrebbero essere stati usati.

Non devi riconoscere l’AI.

Devi rallentare la richiesta.

La regola più importante

Una voce familiare può essere vera.

Può anche essere imitata.

Per questo la sicurezza non deve dipendere dall’orecchio, ma dal processo.

Se una persona cara ha davvero bisogno, sopporterà un minuto di verifica. Se un collega ti sta chiedendo un’azione urgente e legittima, potrà confermarla su un canale ufficiale. Se una banca o un ente ti contatta davvero, non ti chiederà password, codici o pagamenti improvvisi dentro una telefonata emotiva.

La voce può convincere.

Il metodo deve controllare.