Il telefono, la sua voce

13 MAGGIO 2025

L'IA STA DIVENTANDO pervasiva: lo sappiamo bene, lo sapete bene, lo sanno ancora meglio i malfattori. Un nuovo tipo di truffa telefonica che usa la tecnologia per ingannarti con la riproduzione fedele di voci a te familiari potrebbe presto prendere di mira il tuo telefono.

AI truffatore non serve altro se non un piccolo campione della voce, gli basta un frammento di un vocale WhatsApp per creare un robocall IA.

Poi uno che giureresti essere tuo figlio ti chiama e ti racconta “Ciao, sono Filippo, ho avuto un piccolo incidente qui in Umbria. Niente di grave, ma mi servono subito 300 Euro per la riparazione della moto e non ho abbastanza contante.”

Come non abboccare? Tuo figlio Filippo è in vacanza in Umbria e 300 Euro non sono gran cosa per te. Il fatto è che per fortuna Filippo non ha avuto alcun incidente, non è lui al telefono e tu stai per cadere vittima della *truffa dell’impostore*, resa ancora più convincente dalla tecnologia IA.

Riesci solo a immaginare le implicazioni, per esempio in una competizione elettorale? Un noto politico, che appare giornalmente in TV e di cui ben conosci la voce, ti chiama al cellulare e ti spinge a non andare a votare. Non è fantascienza, è già veramente accaduto con una registrazione IA dell’ex presidente USA Biden, che scoraggiava i votanti del New Hampshire dal partecipare alle primarie.

La tecnologia per questo tipo di truffe esiste oggi a costi molto bassi.

L’*impersonation*, ossia la sostituzione di persona, presenta aspetti che possono configurarla come reato nel nostro ordinamento giuridico, ma per stare sul pratico ecco alcuni consigli di prevenzione e difesa.

- Il più ovvio e contemporaneamente più efficace è quello di riagganciare e chiamare direttamente per verifica il congiunto o l’amico che ti ha detto di avere problemi. Non credere che sia così scontato, i truffatori sanno come metterti pressione e non darti il tempo di riflettere.
- Molto importante è acquisire consapevolezza e prestare attenzione ai soliti segnali sospetti, come la provenienza da numeri sconosciuti (spesso con prefissi stranieri), richieste di denaro, pretese di urgenza. A livello aziendale ci sono ottimi corsi di *awareness*, vedi il nostro Cybertraining.
- Può essere utile dotarsi di un’app di protezione come Truecaller.

PS – Ti interessano questi contenuti? Ci piacerebbe sapere che cosa ne pensi. Se credi, visita il nostro sito e resta in contatto

Marcello Fontana
commerciale@gotech.it
+39 351 4272010