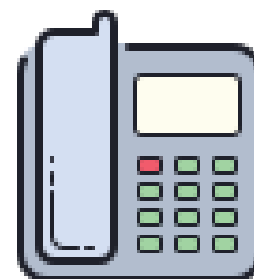


CYBER SECURITY TIPS #26

DEEP FAKE AUDIO: LA MINACCIA DEL FUTURO.



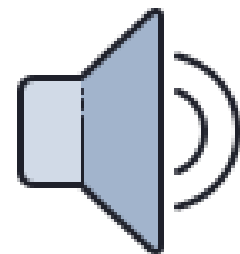
LEGGI SUBITO LE NOSTRE TIPS!



1. COS'È UN DEEP FAKE AUDIO?

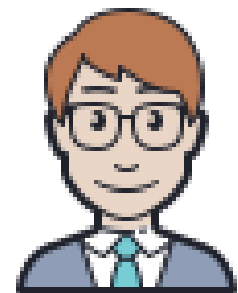
È una nuova tecnica usata dai criminali informatici.

Il Deep Fake Audio sfrutta una tecnologia di intelligenza artificiale per riprodurre la voce umana, al fine di estorcere denaro o dati importanti.



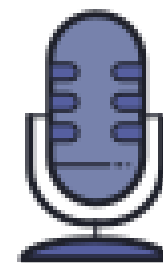
2. L'HACKER PUÒ ASSUMERE LA VOCE DEL TUO CAPO.

La tecnica del Deep Fake Audio è una minaccia in quanto permette all'hacker di fingersi il tuo capo e richiederti, per esempio, di trasferire una cospicua somma di denaro su un conto in banca.



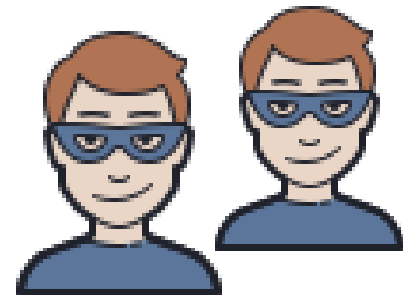
3. È PIÙ SEMPLICE DEL PREVISTO.

Reperire un campione della voce del CEO di un'azienda è relativamente facile per un criminale. Basta cercare un video di un intervento pubblico online oppure intercettare le telefonate.



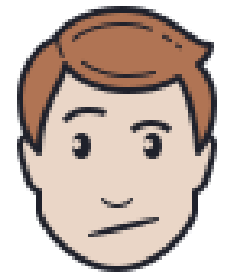
4. L'AI È IN CONTINUA EVOLUZIONE.

La tecnologia di Intelligenza Artificiale che permette il ricalco della voce è in continua evoluzione e potrebbe diventare in breve tempo accessibile a un vasto numero di malintenzionati.



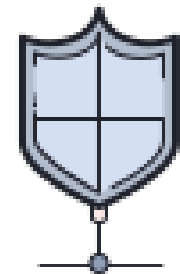
5. L'ERRORE UMANO.

Il Deep Fake Audio rappresenta una minaccia in quanto va a colpire l'anello più debole della sicurezza informatica: le persone. Consente infatti ai criminali di far leva sulla fiducia, il timore e il senso del dovere.



6. È UNA TECNICA CHE SCAVALCA LE VPN.

Il Deep Fake Audio è pericoloso perché scavalca le normali difese aziendali come Firewall e VPN. La buona notizia è che gli esperti stanno già studiando una tecnologia in grado di rilevare questa minaccia.



7. PAROLA D'ORDINE: CYBER SECURITY AWARENESS.

Nel frattempo, occorre sensibilizzare le persone sul pericolo dei Deep Fake Audio e insegnar loro come reagire. Per esempio, se ricevi una telefonata strana dal tuo capo, riaggancia e richiama per verificarne l'identità!



TI È STATO UTILE QUESTO POST?



Sharing is
Caring

lumit.it