Bitdefender

La clonazione della voce di personaggi famosi: le nuove truffe in rapida diffusione sui social media sfruttano l'Intelligenza artificiale

Lo rivela una ricerca Bitdefender che spiega come le voci di star come Oprah Winfrey, Elon Musk, Jennifer Aniston, tra gli altri, vengano usate per promuovere omaggi costosi come iPhone, seggiolini auto Chicco, aspirapolveri Dyson e borse di Michael Kors con l'obiettivo di truffare i consumatori e sottrarre denaro e informazioni personali

Milano, 15 febbraio 2024 - Bitdefender, leader nell'ambito della sicurezza informatica, annuncia oggi i risultati di una ricerca su una tendenza in rapido aumento diffusa sulle piattaforme di social media che consiste nell'utilizzo della tecnologia per clonare la voce di personaggi famosi da parte dei criminali informatici per truffare i consumatori.

Tra le star incosapevolmente coinvolte in questa campagna organizzata dai criminali informatici ci sono Oprah Winfrey, Elon Musk, Jennifer Aniston, Tiger Woods, Hulk Hogan, lo youtuber Mr. Beast e molti altri. Le loro voci vengono utilizzate per sponsorizzare falsi concorsi, giochi d'azzardo e finte opportunità di investimento. Le truffe sfruttano l'immagine (e la voce) di questi personaggi pubblici per promuovere beni costosi in omaggio come l'ultimo modello di iPhone o MacBook, seggiolini auto Chicco, set di attrezzi DeWalt, aspirapolveri Dyson e borse di Michael Kors o Coach a fronte di spese di spedizione comprese tra i 2 e i 15 dollari.

Per aggiungere credibilità ai loro schemi, i truffatori hanno anche creato siti web simili a quelli di quotidiani conosciuti come, per esempio, quello del The New York Times.

La clonazione vocale si avvale dell'utilizzo di strumenti di intelligenza artificiale per creare copie fasulle della voce di un altro individuo. Questa sofisticata tecnologia utilizza tecniche di deep learning per replicare il modo di parlare di una persona e creare l'audio di una voce umana altamente realistica e convincente. Rispetto alle voci artificiali generate interamente da un computer con sistemi di sintesi vocale ormai obsoleti, la clonazione vocale utilizza la voce reale di un altro individuo per produrre discorsi con una resa realistica rispetto all'originale.

Nonostante i numerosi usi leciti, come la creazione di voci fuori campo e di assistenti vocali personalizzati, doppiaggio per gli attori dei film, aiuto alle persone con problemi di linguaggio, narrazione negli audiolibri, la tecnologia di clonazione vocale viene spesso utilizzata in modo improprio per attività fraudolente.

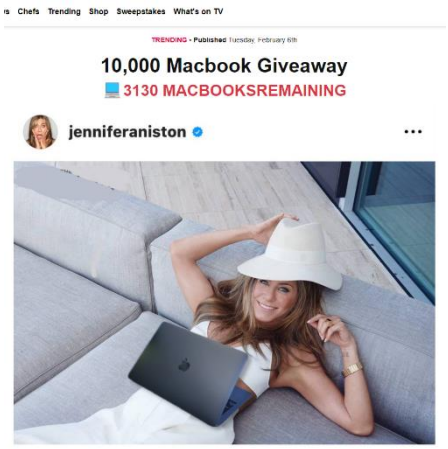
Risultati principali

- L'analisi di Bitdefender stima che queste truffe di clonazione vocale abbiano preso di mira almeno 1 milione di utenti statunitensi ed europei (Romania, Francia, Austria, Belgio, Portogallo, Spagna, Polonia, Svezia, Danimarca, Cipro e Paesi Bassi, tra gli altri). Uno degli annunci ha raggiunto 100.000 utenti ed è stato attivo per alcuni giorni. Tuttavia, le truffe di clonazione vocale non sono limitate alle zone geografiche sopra menzionate. Il fenomeno è molto probabilmente in rapida espansione a livello globale.

- Le truffe di clonazione vocale sponsorizzate dalle star sono presenti sulle piattaforme Meta, tra cui Facebook, Instagram, Audience Network e Messenger, e si rivolgono alla fascia di età compresa tra i 18 e i 65 anni.

- Come per la maggior parte delle truffe online, lo scopo principale è quello di rubare denaro, credenziali e informazioni personali.

- Tutti i video di clonazione vocale analizzati seguono la stessa narrazione: tutti coloro che guardano il video fanno parte di un "gruppo esclusivo di 10.000 individui" che possono acquistare prodotti esclusivi a seguito di un modesto pagamento che parte da 2 dollari (a seconda dell'annuncio/prodotto). Nello screenshot qui accanto e sotto, i truffatori hanno clonato la voce della star di Hollywood Jennifer Aniston.



Come proteggersi

Queste truffe si stanno evolvendo rapidamente e diventano sempre più difficili da individuare man mano che l'intelligenza artificiale compie passi in avanti. Bitdefender consiglia innanzitutto ai consumatori di diffidare delle offerte troppo allettanti per essere vere anche se per sponsorizzarle vengono utilizzate celebrità come testimonial. Altre raccomandazioni specifiche da tenere presente in questi casi:

- **Prestare attenzione alla qualità della voce.** Alcune voci clonate potrebbero avere toni insoliti, essere statiche o presentare incoerenze nel modo di parlare.
- **Rumori di fondo e artefatti:** sebbene la clonazione vocale di alta qualità riduca al minimo i rumori di fondo, potrebbero comunque essere presenti: il suggerimento è quindi quello di ascoltare attentamente se ci sono rumori di fondo insoliti o artefatti digitali.
- **Diffidare di richieste insolite:** fare attenzione se vengono richieste informazioni personali o denaro o domande inconsuete. L'obiettivo delle truffe con clonazione vocale è rubare denaro. È quindi opportuno sempre controllare gli annunci e i video che promettono considerevoli ritorni sugli investimenti, anche se sembrano sponsorizzati da una celebrità, da un influencer dei social media o da un personaggio politico.

Informazioni su Bitdefender

Bitdefender è una società leader nella sicurezza informatica che offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce del mondo. Proteggendo milioni di consumatori, aziende e ambienti governativi, Bitdefender è considerata uno degli esperti più affidabili del settore per eliminare le minacce, proteggere la privacy e i dati, e ottenere la resilienza informatica. Grazie a notevoli investimenti in ricerca e sviluppo, Bitdefender Labs scopre centinaia di nuove minacce ogni minuto e convalida miliardi di query sulle minacce al giorno. L'azienda ha aperto la strada a innovazioni rivoluzionarie in varie tecnologie, come anti-malware, sicurezza IoT, analisi comportamentale e intelligenza artificiale. La sua tecnologia è usata su licenza da più di 180 dei marchi tecnologici più noti al mondo. Fondata nel 2001, Bitdefender ha clienti in oltre 170 paesi con uffici in tutto il mondo. Per maggiori informazioni, visitare https://www.bitdefender.it.

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it