

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6068 di Lunedì 27 aprile 2026

Deepfake: come identificare fotografie e filmati contraffatti

Un'infografica di immediata comprensione, messa a disposizione dell'FBI, aiuterà tutti i nostri lettori a individuare foto e filmati contraffatti, grazie ad applicativi di intelligenza artificiale.

Dopo che lo FBI si è accorto di aver ricevuto centinaia di migliaia di rapporti, afferenti a frodi perpetrate con filmati e fotografie (deepfake) costruiti con intelligenza artificiale, ha ritenuto opportuno mettere a disposizione di tutti cittadini una chiarissima infografica, che aiuta ad individuare questi documenti contraffatti.

Si faccia attenzione che questi applicativi possono contraffare sia fotografie, sia video, sia audio. In genere questi applicativi prendono una foto di un soggetto, conosciuto dal bersaglio dell'attacco, e sono in grado di creare nuove fotografie e filmati, del tutto credibili. In altri casi, come sta avvenendo attualmente in Italia, la contraffazione fa riferimento ad un personaggio pubblico, ritenuto affidabile, che dà consigli di investimenti finanziari tramite visualizzazioni sul Web.

Pubblicità

Ecco le situazioni che aiutano a mettere in evidenza possibili contraffazioni:

- Nell'immagine che viene presentata vi sono alcune caratteristiche facciali che sembrano sfocate o distorte?
- La persona che appare nel filmato sbatte le palpebre con grande frequenza o con bassissima frequenza?
- I capelli ed i denti sono realistici?
- È presente uno slittamento, o mancanza di sincronizzazione, fra audio e video?
- Il tono della voce del soggetto filmato è piatto o comunque ha una intonazione innaturale?
- Nel filmato possono apparire delle ombre, anche in movimento, non giustificate dalla scena ripresa?

Inoltre, il documento raccomanda di fare attenzione anche alle tipologie di richieste che vengono avanzate, come ad esempio la richiesta di denaro, del rilascio di password, di applicazione di pressioni emotive sul destinatario del messaggio, sull'uso di frasi insolite, che la persona coinvolta non ha mai usato prima.

In tutti questi casi, chi risiede negli Stati Uniti può rivolgersi allo FBI, mentre chi risiede in Italia può rivolgersi di preferenza alla polizia postale, che è incaricata di indagare su questa tipologia di reati.

[Vai all'infografica.](#)

Le infografiche di Puntosicuro:

DEEFAKE FRAUDS: HOW TO PROTECT YOURSELF IN THE AGE OF AI



THE IMPACT OF DEEFAKE FRAUDS

4,2 MILLION+

More than 4.2 million fraud reports. Reports received by the FBI since 2020 due to the increase in cybercrime.

50,5 BILLION

\$50.5 billion in losses. The enormous total economic cost resulting from fraudulent activities reported in recent years.

WHAT ARE DEEFAKES?

Images, videos, or audio generated or tampered with by AI to simulate real people and gain the trust of victims.

HOW TO DETECT A DEEFAKE



ANALYZE FACIAL FEATURES

Look for facial characteristics that are blurred, distorted, or occur at an unnatural frequency (too frequent or absent).



CHECK PHYSICAL DETAILS AND SHADOWS

Check if the hair, teeth, and facial shadows look real and consistent with the lighting in the video.



EVALUATE AUDIO-VIDEO CONSISTENCY

Pay attention if the audio is out of sync with lip movements, labored, or if the voice sounds flat or robotic.

WARNING SIGNS (RED FLAGS)



EMOTIONAL MANIPULATION

Requests that exploit fear or create a sense of urgency to pressure immediate action.



UNEXPECTED REQUESTS FOR MONEY OR DATA

Requests for passwords, personal information, or transfers of money under the pretext of secrecy.



COMMUNICATION OUTSIDE NORMAL CHANNELS

Messages or calls from contacts who use unusual language or an uncharacteristic tone.

TIPS FOR STAYING SAFE



PAUSE AND REFLECT

Don't rush; verify the identity of the sender through official channels or by using trusted phone numbers.



CREATE A FAMILY PASSWORD

Agree on a secret code with your loved ones to confirm their identity in case of suspicious calls.



LIMIT YOUR DIGITAL FOOTPRINT

Reduce the publication of photos and online vocal clips, which can be used to train deepfake models.

HOW TO REPORT



REPORT TO THE FBI (IC3.GOV)

Officially report fraud attempts and cybercrime to the FBI's Internet Crime Complaint Center.



NOTIFY YOUR BANK AND LOCAL POLICE

If you have sent money, contact your financial institution immediately to try to block the transactions.

TRUFFE DEEFAKE: COME PROTEGGERSI NELL'ERA DELL'IA



L'IMPATTO DELLE TRUFFE DEEFAKE

4,2 MILIONI+

Oltre 4,2 milioni di denunce di frode. Rapporti ricevuti dall'FBI a partire dal 2020 a causa dell'aumento dei crimini informatici.

50,5 MILIARDI

50,5 miliardi di dollari di perdite. L'enorme costo economico totale derivante dalle attività fraudolente segnalate negli ultimi anni.

COSA SONO I DEEFAKE?

Immagini, video o audio generati o manipolati dall'IA per simulare persone reali e guadagnare la fiducia delle vittime.

COME RILEVARE UN DEEFAKE



ANALIZZA I TRATTI SOMATICI

Cerca caratteristiche facciali sfocate, distorte o una frequenza di ammicciamento degli occhi innaturale (troppo frequente o assente).



VERIFICA I DETTAGLI FISICI E LE OMBRE

Controlla se i capelli e i denti sembrano reali e se sono presenti ombre insolite o asimmetriche nel video.



VALUTA LA COERENZA AUDIO-VIDEO

Fai attenzione se l'audio è fuori sincrono rispetto al movimento della labbra o se il tono della voce risulta piatto e robotico.

SEGNALI DI ALLARME (RED FLAGS)



MANIPOLAZIONE EMOTIVA

Richieste che sfruttano la paura o creano un senso di urgenza estrema per spingere all'azione immediata.



RICHIESTE INASPETTATE DI DENARO O DATI

Sollecitazioni insolite per password, informazioni personali o trasferimenti di denaro sotto il vincolo della segretezza.



COMUNICAZIONE FUORI DAL COMUNE

Messaggi o chiamate da conoscenti che usano un linguaggio o un tono non coerente con la loro personalità.

CONSIGLI PER LA SICUREZZA



FERMATI E RIFLETTI

Non lasciarti pressare; verifica sempre l'identità del richiedente tramite canali ufficiali o numeri di telefono fidati.



CREA UNA PAROLA D'ORDINE FAMILIARE

Stabilisci un codice segreto con i tuoi cari per confermare la propria identità in caso di chiamate sospette.



LIMITA L'IMPRONTA DIGITALE

Riduci la pubblicazione di foto e clip vocali online, poiché possono essere usate per addestrare modelli di deepfake.

COME SEGNALARE



CONTATTA L'FBI (IC3.GOV)

Segnala ufficialmente il tentativo di frode alle autorità competenti per la criminalità informatica.



AVVISA LA TUA BANCA E LA POLIZIA LOCALE

Se hai già inviato denaro, contatta immediatamente il tuo istituto finanziario per bloccare le transazioni.

clicca sulle immagini per ingrandirle

Adalberto Biasiotti



Licenza Creative Commons