Deep fake, la nuova arma dei truffatori online

In questi giorni è venuta alla luce una presunta truffa online di proporzioni enormi, che ha coinvolto migliaia di utenti ignari. La polizia postale, in collaborazione con la security di Eni, ha bloccato e oscurato più di 400 siti web che pubblicizzavano presunti falsi investimenti su piattaforme di trading online. Questi siti promettevano guadagni facili e veloci, ma in realtà si sarebbe trattato di una finta società di investimento che usava il logo e le immagini dei dirigenti dell'Eni senza autorizzazione. Per rendere più credibile la sua associazione con il gigante dell'energia nazionale, la società avrebbe utilizzato programmi di intelligenza artificiale per creare video deep-fake, in cui si vedevano presunti esperti e testimonial che elogiavano le opportunità di investimento.

Senza entrare nel merito della vicenda, di cui non si conoscono gli esatti contenuti, la suddetta operazione consente di svolgere considerazioni di carattere generale sul fenomeno delle offerte di investimenti online, che sono sempre più diffuse e allettanti, ma possono nascondere delle trappole pericolose, nonché su alcune tematiche di carattere squisitamente giuridico.

Il trading online può essere un'attività redditizia e appassionante, ma comporta anche dei rischi che non vanno sottovalutati.

La prima criticità riguarda la mancanza di trasparenza e di regolamentazione. Molte piattaforme di trading online operano senza autorizzazione e senza rispettare le norme vigenti, rendendo difficile il controllo e la tutela dei consumatori.

Inoltre, spesso non forniscono informazioni chiare e complete sulle condizioni, i costi e i rendimenti degli investimenti, esponendo gli utenti a sorprese spiacevoli. Per evitare di cadere in trappole è importante verificare sempre la reputazione e l'affidabilità della piattaforma scelta, consultando le recensioni, i pareri e le esperienze di altri utenti, e controllando che sia autorizzata e regolamentata dagli enti competenti. Inoltre, alcune piattaforme di trading online usano tecniche sofisticate per ingannare e convincere gli utenti a investire sempre di più, come la creazione di falsi testimonial, la falsificazione di dati e grafici, l'uso di robot e algoritmi che influenzano le decisioni, la creazione di falsi contatti e assistenti. Per difendersi da queste pratiche scorrette e illegali, è fondamentale essere sempre informati e consapevoli, non farsi abbindolare da promesse irrealistiche o da pressioni psicologiche, e denunciare eventuali situazioni sospette o anomale alle autorità competenti.

Infine rileva la volatilità e l'incertezza dei mercati. Gli investimenti online sono spesso legati a mercati altamente speculativi e instabili, come le criptovalute, le opzioni binarie, il forex, ecc. Per limitare questi pericoli, è essenziale avere una buona preparazione e una solida strategia, basarsi su analisi e dati affidabili, diversificare il portafoglio, impostare dei limiti di perdita e di guadagno, e non investire mai più di quanto si può permettere di perdere.

Sul piano giuridico, l'operazione di polizia appena compiuta, mette al centro i temi dell'utilizzo dell'intelligenza artificiale per creare video deep-fake e del sequestro dei siti web.

I deepfake sono dei prodotti digitali che usano l'intelligenza artificiale per modificare video o immagini esistenti, sovrapponendo volti o voci di altre persone. Il risultato è un contenuto che inganna lo spettatore, facendogli credere che

sia autentico. Per esempio, si potrebbe creare un video in cui una celebrità dice qualcosa che non ha mai detto, o in cui una persona comune appare in una situazione compromettente.

Spesso, i deepfake vengono usati per divertimento o per creare delle parodie, ma non sono sempre innocui, potendo avere delle ripercussioni molto gravi, che riguardano diversi aspetti della vita delle persone coinvolte.

Uno di questi è la privacy. Se si usa il volto o la voce di una persona senza il suo consenso, si viola la sua privacy. Questo può essere molto dannoso, soprattutto se il deepfake la mostra in una situazione imbarazzante o illegale, come ad esempio in un video pornografico o in un reato. La persona potrebbe subire delle molestie, delle minacce o dei ricatti, oltre a un danno alla sua immagine e alla sua dignità. Un altro è la diffamazione. Un video falso potrebbe far credere che qualcuno abbia fatto o detto qualcosa di sbagliato o di offensivo, come ad esempio una dichiarazione politica, una confessione, una truffa o un insulto. La persona o l'azienda potrebbe subire, oltre alla lesione della propria onorabilità e credibilità, delle perdite economiche e delle azioni legali.

Un terzo aspetto è l'inganno del pubblico. Se si usa il deepfake per scopi fraudolenti o per diffondere notizie false, si inganna il pubblico e si influenzano le sue opinioni. Un video falso potrebbe alterare la verità su un fatto storico, politico o sociale, come ad esempio una guerra, una elezione, una manifestazione o una catastrofe. Il pubblico potrebbe essere indotto a credere a delle bugie, a prendere delle decisioni sbagliate o a sostenere delle cause ingiuste.

Altra questione attiene alla proprietà intellettuale. Se si usa il deepfake per sfruttare i diritti d'autore o i marchi registrati di altre persone, si viola la loro proprietà intellettuale. Chi ha i diritti su un contenuto falso? L'autore originale, il creatore del deepfake o nessuno dei

due?

Tema non trascurabile è quello della imputazione della responsabilità. Se si crea o si diffonde un deepfake, chi ne è responsabile? Solo l'autore o anche la piattaforma che lo ospita ? Questa è un'altra questione molto delicata, che richiede una collaborazione tra i diversi attori coinvolti. L'autore dovrebbe essere identificato e punito, la piattaforma dovrebbe rimuovere il contenuto e avvisare le autorità, e le vittime dovrebbero essere tutelate e risarcite.

Quanto al sequestro dei siti web, è una misura cautelare che le autorità giudiziarie possono adottare quando sospettano che un sito web ospiti contenuti illegali. Si tratta di una forma di intervento diretto sui provider di servizi internet, che vengono obbligati a impedire ai propri utenti di accedere al sito o alla pagina web incriminata. Per farlo, i provider realizzano sistemi di filtraggio basati sui DNS (Domain Name System) o sugli IP (Internet Protocol), che rendono inaccessibile il dominio o l'indirizzo del sito.

Tuttavia, tale misura non è sempre semplice da attuare, soprattutto quando il sito si trova all'estero ma è raggiungibile dall'Italia. In questo caso, le autorità italiane devono affrontare questioni di giurisdizione e cooperazione internazionale. Possono adottare diverse strategie, come il blocco dei DNS nella rete nazionale, la collaborazione con le autorità del paese estero o il ricorso a trattati internazionali che prevedono assistenza giuridica reciproca.

Il sequestro dei siti web è, pertanto, una misura, che presenta vari problemi, sia dal punto di vista pratico che giuridico. Tra le sfide più comuni, possiamo citare la localizzazione e la giurisdizione del sito, il rispetto dei diritti fondamentali, la tecnica e l'implementazione del blocco e i rischi di censura e abuso.

La localizzazione e la giurisdizione del sito possono essere difficili da determinare con precisione, complicando l’applicazione delle misure cautelari. Inoltre, quando il sito è ospitato all’estero, le autorità devono fare affidamento sulla cooperazione internazionale, che non è sempre garantita o tempestiva.

Il rispetto dei diritti fondamentali implica il bilanciamento tra la tutela dei diritti delle vittime e il rispetto per la libertà di informazione e opinione.

Il sequestro dei siti web è, quindi, un’arma a doppio taglio: può essere uno strumento efficace per contrastare reati online, ma richiede attenzione e cautela per evitare effetti indesiderati.

https://www.key4biz.it/deep-fake-la-nuova-arma-dei-truffatori-online/481274/