

Finti video e trappole al Nasdaq. Come le reti criminali usano l'AI e i social per clonare gli esperti di Borsa

LINK: <https://www.money.it/finti-video-e-trappole-al-nasdaq-come-le-reti-criminali-usano-l-ai-e-i-social-per-clonare-gli-esperti-di-borsa>

Finti video e trappole al Nasdaq. Come le reti criminali usano l'AI e i social per clonare gli esperti di Borsa Redazione Dalle sponsorizzate social ai gruppi privati WhatsApp: la guida per smontare le truffe deepfake che abusano dell'immagine di **Salvatore Gaziano** e di noti analisti. Come funziona lo schema Pump & Dump sulle azioni americane e i campanelli d'allarme per proteggere i risparmi. - di **Salvatore Gaziano**. Nel 1929 il pittore surrealista René Magritte dipinse una pipa con la celebre scritta: Ceci n'est pas une pipe (Questa non è una pipa). Voleva ricordarci che la rappresentazione visiva di un oggetto non è l'oggetto reale. Oggi quella lezione d'arte è la prima regola di sopravvivenza nella finanza digitale. Ve lo dico da vittima diretta di un pesante furto d'identità: da settimane circolano sui social network decine di annunci abusivi che utilizzano il mio volto e la mia voce. Quando vedete un video sponsorizzato su Facebook, Instagram o TikTok in cui il sottoscritto vi invita a entrare in un gruppo WhatsApp per ricevere consigli di Borsa "esclusivi", quello non è

Salvatore Gaziano. È un deepfake: un clone digitale creato da truffatori tramite l'AI per rubare l'identità e la reputazione di consulenti e professionisti reali e usarla come esca contro i risparmiatori. Non è un caso isolato. In tutto il mondo, economisti, giornalisti e imprenditori riconosciuti vengono sistematicamente colpiti per "vampirizzarne" la credibilità. Tra le voci più autorevoli che hanno denunciato questo cortocircuito c'è Milena Gabanelli, che ha definito il fenomeno un raggio internazionale costruito sui volti di personaggi pubblici dotati di credibilità, accusando Meta di incassare i proventi delle inserzioni senza rispondere delle conseguenze. Come emerge da un'intervista del Financial Times al presidente del FATF Giles Thomson, basata anche su dati Interpol, le reti criminali stanno abbandonando i grandi centri di frode per operare attraverso "micro-celle" di una o due persone gestite con l'AI. Le truffe potenziate dall'intelligenza artificiale risultano 4,5 volte più redditizie di quelle tradizionali, in un fenomeno

che vale circa 500 miliardi di dollari l'anno. La novità non è solo tecnologica, ma psicologica: non occorre inventare un investimento falso, basta falsificare chi lo consiglia. Il gancio deepfake: l'autorevolezza rubata. L'inganno parte dai social. Tramite sponsorizzate a pagamento, i truffatori utilizzano video e audio clonati di analisti o consulenti reali. Il deepfake è il dispositivo di acquisizione: promette analisi riservate e indirizza le vittime dentro gruppi WhatsApp o Telegram, gli "Investment Club" abusivi o "circoli di investimento" denunciati dall'FBI. Qui scatta il condizionamento psicologico basato sulla falsa "riprova sociale": bot e complici pubblicano quotidianamente screenshot di finti guadagni e ringraziamenti al "maestro". Finte segretarie del personaggio "vampirizzato" invitano ad aumentare la posta e inviano vocali sintetici o report di analisi generati in serie tramite chatbot e motori di IA. Dal video alla Borsa reale: la trappola delle azioni "esca". A differenza delle vecchie truffe con broker fittizi, dove le vittime venivano invitate a spostare i soldi

verso piattaforme estere non regolamentate, le frodi più recenti spingono l'utente a operare sul proprio conto titoli personale, presso la banca abituale. L'investimento sembra sicuro perché il mercato è reale e, apparentemente, il denaro non lascia l'istituto di fiducia dell'investitore. I truffatori orientano le vittime verso micro-cap quotate al Nasdaq Capital Market o al NYSE: società con capitalizzazione ridottissima, bilanci in sofferenza e bassissima liquidità. L'ingranaggio si sviluppa in cinque fasi. 1) L'accreditamento e l'esca del piccolo guadagno Nei primi giorni il finto consulente, che chi legge crede sia quello vero, parla di temi generali e titoli primari per rafforzare la fiducia. Poi sposta il focus su una micro-cap poco liquida, indicando un primo acquisto che si chiude spesso con un piccolo profitto dimostrativo, per esempio un +10%, così da conquistare una fiducia cieca e stimolare la paura di perdere un'opportunità ancora più grande. 2) La manipolazione a compartimenti stagni I risparmiatori catturati dai social vengono distribuiti in decine di gruppi WhatsApp separati e privi di contatto tra loro. Questa architettura consente ai truffatori di

gestire il mercato: possono ordinare al Gruppo A di acquistare, creando la spinta sui prezzi, e al Gruppo B di vendere, usando la liquidità dei nuovi arrivati per far realizzare il "finto guadagno" al secondo gruppo. Inoltre, se un gruppo viene chiuso, l'albero non crolla e gli altri canali continuano a operare. 3) La trappola dello screenshot e della finta commissione I gestori chiedono la prova dell'ordine d'acquisto con la contabile bancaria, spiegando che il loro compenso sarà solo una commissione del 5% sui profitti futuri, da corrispondere solo dopo l'incasso. Questa mossa psicologica fa credere alla vittima di condurre il gioco e di trovarsi di fronte a un professionista onesto, mentre in realtà consegna ai truffatori la mappa esatta del capitale che può mobilitare. 4) L'up-sell da 50.000 euro Dimostrata la presunta infallibilità del "maestro", scatta l'affondo. I gestori della chat chiedono di alzare drasticamente la posta, sollecitando l'impiego di somme ingenti, anche 50.000 euro o più, sulla "prossima operazione imperdibile". Se si comprende che la vittima ha patrimoni importanti, l'asticella viene alzata ulteriormente. 5) Il Pump & Dump finale e lo scarico La

rete criminale ordina l'acquisto coordinato del titolo a migliaia di utenti sparsi nelle varie chat. Gli acquisti al dettaglio concentrati nello stesso momento spingono artificialmente in alto la quotazione (Pump). Nel momento di massimo picco, chi possiede la maggior parte delle azioni a prezzi stracciati le scarica sul mercato in un unico blocco (Dump), provocando il crollo istantaneo del titolo, anche dell'80% o del 90% in pochi minuti. Così funzionano le frodi Pump & Dump: una catena di Sant'Antonio finanziaria in cui le vittime vedono il capitale polverizzato in poche ore. Che succede dopo? Dopo il crollo, i truffatori spiegano che si è verificato un evento "inaspettato" di mercato e offrono nuovi consigli per "recuperare" le perdite, spingendo la vittima verso un indebitamento ancora maggiore. Chi finisce in questi elenchi rischia poi di cadere nella seconda truffa, il recovery scam: a distanza di settimane la vittima viene ricontattata da finti "studi legali internazionali" o "esperti di recupero crediti" che promettono di recuperare le somme perse in cambio di un pagamento anticipato. Si tratta esattamente delle stesse organizzazioni criminali. I 6 campanelli d'allarme e le

regole di autotutela Per un risparmiatore o un trader è fondamentale saper individuare i segnali d'allarme oggettivi. 1) La falsa sicurezza del nome o delle spunte di "verifica" Le piattaforme social non verificano se la pagina che promuove la campagna sia quella reale o una sua copia. Esistono inserzioni con nomi di fantasia, ma anche pagine clonate con nome e cognome reale del consulente e finte spunte di "verifica". L'attuale sistema non effettua controlli sull'identità reale di chi compra annunci pubblicitari finanziari. Non bisogna mai fidarsi dell'annuncio: la fonte va verificata unicamente tramite i profili e i siti ufficiali del professionista o i recapiti OCF e Consob. 2) L'invito "selvaggio" su WhatsApp o Telegram Nessun consulente iscritto all'Albo OCF fornisce segnali di trading in gruppi di messaggistica, in modo non tracciato e privo di garanzie. La consulenza reale avviene solo ed esclusivamente tramite rapporti contrattuali formalizzati e accompagnati dai disclaimer di legge. 3) Promesse di rendimenti spropositati o garanzie anti-perdita Slogan che promettono guadagni del 300% o del 500%, o la "copertura delle perdite", sono un indice matematico

di frode. 4) Richiesta dello screenshot dell'eseguito L'obbligo di inviare la contabile bancaria serve solo ai truffatori per verificare quanto capitale la vittima è in grado di mobilitare. 5) Pressione all'acquisto "al meglio" su micro-cap USA L'ordine perentorio di acquistare con urgenza piccole società estere sconosciute al prezzo di mercato è la spia classica del Pump & Dump. Mai acquistare titoli senza una rigorosa due diligence: queste micro-cap hanno spesso sede in giurisdizioni offshore come le Isole Cayman, operatività fuori dagli Stati Uniti, quotazione come Foreign Private Issuer, rischio di delisting e bilanci opachi. 6) L'intelligenza artificiale come primo filtro, ma con avvertenza Interrogando i modelli di IA con domande dirette, del tipo "il consulente X sta consigliando azioni su WhatsApp?", si ottiene spesso un'immediata smentita. Non è però una panacea infallibile: in futuro le reti criminali tenteranno sempre più di inquinare i dati del web (AI data poisoning) per condizionare gli algoritmi. L'antidoto definitivo resta la verifica diretta sui canali ufficiali del professionista o sui registri OCF e Consob. I social non garantiscono nulla. Serve una verifica preventiva sugli

inserzionisti Per evitare che altri risparmiatori cadano in trappola, è fondamentale comprendere questi meccanismi di pressione psicologica e frode informatica. Più risparmiatori sono informati, meno queste truffe funzioneranno. Da parte mia ho formalizzato tutte le denunce, le segnalazioni e le diffide nelle sedi competenti. La vicenda, tuttavia, va ben oltre il mio singolo caso: sono tantissimi i consulenti, i giornalisti e i professionisti colpiti da queste frodi deepfake in Italia e nel mondo. E mentre in Italia e in Europa si parla continuamente di tutelare i minori dalle insidie dei social, ci si dimentica troppo spesso dei "maggiori". L'attuale regolamentazione europea sembra nei fatti aver abdicato alla propria sovranità digitale a favore delle Big Tech, consentendo loro di fare il bello e il cattivo tempo senza rispondere dei danni generati a monte, protette da vecchi scudi normativi di esenzione e da procedure oggi del tutto anacronistiche di fronte all'avvento dell'intelligenza artificiale. Si fa quindi quanto mai urgente un intervento che imponga alle grandi piattaforme digitali obblighi di verifica preventiva e stringente

(Know Your Advertiser) sull'identità e sulle autorizzazioni di chi acquista pubblicità in ambito finanziario: una misura indispensabile per proteggere il mercato, la legalità e la trasparenza verso i cittadini e i risparmiatori. **Salvatore Gaziano** è consulente finanziario indipendente iscritto all'Albo OCF, direttore investimenti di **SoldiExpert SCF** e giornalista professionista.