MalpensaNews

Truffe generate dall’AI: quando non puoi più fidarti di quello che vedi

divisionebusiness · Monday, April 20th, 2026

Fino a poco tempo fa, individuare una truffa era relativamente semplice. Errori nel testo, incongruenze grafiche o richieste poco credibili rappresentavano dei segnali abbastanza chiari. Oggi, invece, questi elementi sono sempre meno frequenti. L’intelligenza artificiale ha reso le frodi digitali più sofisticate. I contenuti risultano coerenti, ben costruiti e spesso basati su informazioni reali, rendendo maggiormente complesso distinguerli da comunicazioni legittime. Nel 2025, secondo Vectra AI, le truffe basate sull’AI sono aumentate di ben il 1.210%. In questo contesto, la prevenzione richiede un approccio più strutturato, basato sulla verifica, la consapevolezza e l’uso di strumenti adeguati.

Perché le truffe AI sono così difficili da individuare?

Le truffe tradizionali presentavano spesso dei segnali evidenti: errori nel testo, loghi di bassa qualità, traduzioni poco accurate. Elementi che, con un minimo di attenzione, permettevano di individuare facilmente il rischio. Oggi questi indizi sono sempre meno presenti.

Secondo IlSoftware.it, il 48% delle truffe potenziate dall’AI riesce già a superare i filtri di sicurezza standard. I contenuti risultano curati, coerenti e credibili, sia dal punto di vista visivo che comunicativo.

La differenza sta anche nel modo in cui queste truffe vengono costruite. I sistemi di intelligenza artificiale sono in grado di replicare il tono, lo stile e le modalità espressive di persone reali, spesso appartenenti alla sfera personale o professionale della vittima.

Un messaggio che sembra arrivare dal proprio responsabile, una chiamata con la voce di un familiare, un volto noto associato a un’opportunità di investimento. In questi contesti, la fiducia diventa un fattore critico. La familiarità del contenuto riduce la percezione del rischio e porta a reagire con maggiore rapidità, limitando le verifiche.

Deepfake, voice cloning e phishing personalizzato: come funzionano?

Le truffe basate sull’intelligenza artificiale stanno crescendo rapidamente, anche in Italia. I dati più recenti aiutano a inquadrare meglio la dimensione del fenomeno:

- +1.210% truffe AI a livello globale

- +300% truffe deepfake
- +456% casi di voice cloning in Italia
- fino al 54% di click rate nel phishing personalizzato

Deepfake: quando il video sembra reale

I deepfake vengono creati a partire da contenuti pubblici, come foto e video disponibili sui social, che vengono rielaborati per ricostruire il volto e le espressioni con un alto livello di precisione. Il risultato è un video estremamente realistico, difficile da distinguere da uno autentico.

Anche in Italia si sono già verificati dei casi concreti. Video falsi con Carlo Cracco e Chiara Ferragni sono stati utilizzati per promuovere delle piattaforme di investimento inesistenti, spesso tramite inserzioni sui social.

Voice cloning: la voce diventa una prova falsa

Il voice cloning consente di replicare una voce a partire da pochi secondi di audio, ad esempio un vocale o un video pubblicato online. Il risultato può essere estremamente realistico, al punto da risultare credibile anche in situazioni sensibili.

In Italia, secondo la Polizia Postale, i casi segnalati sono cresciuti del 456% tra il 2024 e il 2025.

Un episodio rilevante ha coinvolto anche delle figure istituzionali. Alcuni imprenditori sono stati, infatti, contattati con una voce attribuibile al Ministro della Difesa Guido Crosetto, accompagnata da richieste di bonifici urgenti. In almeno un caso, il trasferimento ha superato il milione di euro.

Phishing personalizzato: messaggi costruiti su misura

Il phishing si è evoluto in modo significativo. I modelli di intelligenza artificiale analizzano i profili social, le abitudini digitali e i comportamenti online al fine di costruire dei messaggi coerenti con il contesto della persona che li andrà a ricevere.

Email, SMS e messaggi su app risultano plausibili, con riferimenti realistici e un tono adeguato alla situazione. Questo aumenta la probabilità di interazione: alcune campagne analizzate da Vectra AI hanno registrato dei tassi di clic fino al 54%, nettamente superiori rispetto al phishing tradizionale.

Ne deriva una modalità di attacco più mirata, basata su dati e relazioni, in grado di ridurre sensibilmente i segnali di allarme.

Come verificare i contenuti e proteggersi online?

La prima difesa è operativa: fermarsi qualche secondo prima di reagire. Le truffe più efficaci fanno, infatti, leva sull’urgenza e l’emotività.

Alcune abitudini aiutano a ridurre in modo concreto il rischio:

- Definire una parola d’ordine con i familiari: in caso di chiamate che segnalano delle situazioni di emergenza, è utile richiedere la parola concordata. In presenza di esitazioni o di risposte incoerenti, conviene interrompere la conversazione.
- Verificare sempre attraverso i canali ufficiali: per richieste urgenti da parte di banche, aziende o enti pubblici, è preferibile chiudere la comunicazione e ricontattare autonomamente i riferimenti

ufficiali.
- Analizzare con attenzione i contenuti video e audio: segnali come movimenti delle labbra poco naturali, asincronie audio o delle anomalie nell'illuminazione possono indicare manipolazioni.
- Limitare la condivisione di contenuti personali: foto, video e registrazioni vocali pubblicate online possono essere riutilizzate per costruire attacchi mirati.

Un aspetto spesso trascurato riguarda la sicurezza della navigazione. Quando ti colleghi a reti Wi-Fi pubbliche o poco protette, i dati possono essere intercettati e utilizzati per raccogliere informazioni utili a rendere gli attacchi più credibili.

In questo contesto, una VPN consente di cifrare il traffico internet e di mascherare l'indirizzo IP, riducendo le possibilità di tracciamento e profilazione. Se stai valutando questa soluzione, confrontare i prezzi delle VPN disponibili è un buon punto di partenza: i piani a lungo termine possono scendere anche sotto i 2 € al mese, mentre gli abbonamenti mensili arrivano fino a 10-15 €.

Conclusione

L'intelligenza artificiale non ha introdotto nuove tipologie di truffa, ma ha reso quelle esistenti molto più difficili da individuare. Affidarsi esclusivamente all'intuito non è più sufficiente: serve un approccio maggiormente strutturato, basato su verifiche, consapevolezza e strumenti adeguati.

La difesa resta possibile, ma dipende dal tempismo. Fermarsi a controllare, verificare le richieste e gestire con cautela le situazioni urgenti permette di ridurre in modo concreto il rischio.

This entry was posted on Monday, April 20th, 2026 at 6:00 am and is filed under Scienza e Tecnologia
You can follow any responses to this entry through the Comments (RSS) feed. You can skip to the end and leave a response. Pinging is currently not allowed.