Quando vi innamorate… di un avatar

Stamattina mi è capitato un reel curioso su Facebook: Una bella donna, non molto vestita, molto ammiccante, invita a contattarla. Fin qui nulla di nuovo.

La differenza è che nel video c'era scritto chiaramente che era stato creato con "HeyGen", una piattaforma di intelligenza artificiale per creare avatar realistici.

E infatti si vedeva benissimo: movimenti un po' artificiali, doppiaggio sintetico, espressioni perfette.

L'account pubblica solo questo tipo di reel.

Per curiosità ho scritto sotto al video:

"Attenzione: vi state innamorando di un avatar creato con l'intelligenza artificiale."

Tempo due secondi e mi arriva automaticamente questo messaggio:

"Ehi Claudio!! Grazie per il tuo commento! Ho visto la tua attività sotto la foto e devo dirti che la ragazza dello scatto ha notato proprio te.
Le piacerebbe parlarti, ma preferisce farlo in un posto più privato.
Ti sta aspettando sul portale di incontri – lì potrete conoscervi meglio e magari scambiarvi i numeri."

Tradotto: non è una persona, è un bot automatico e l'obiettivo è portarti fuori da Facebook.

A quel punto cosa succede?

Succede quasi sempre questo schema:

1. Ti registri sul sito di incontri (spesso pagando o lasciando dati personali)

2. Inizia a scriverti la "ragazza" che è quasi sempre un operatore o un altro bot

3. La conversazione diventa sempre più flirtante o provocante

4. A un certo punto ti chiedono di: comprare crediti per continuare a scrivere pagare una chat privatapagare per scambiare il numero oppure iscriversi a servizi premium.

E da lì il portafoglio si svuota velocemente.

La cosa interessante però non è la truffa in sé. Quelle esistono da vent'anni.

La novità è questa: oggi le truffe hanno il volto dell'intelligenza artificiale.

Non più foto rubate su internet, ma persone completamente inventate, che: sorridono, parlano, fanno video, sembrano assolutamente reali.

E molti utenti non si accorgono di nulla.

Quindi piccolo consiglio del mattino:

“Se una donna bellissima sui social vi scrive dopo 30 secondi dicendo che ha notato proprio voi… non avete trovato l’amore, avete trovato un algoritmo molto ben programmato! “

Da annotarsi:

L’avatar non è più solo un video

Prima c’era solo il reel seducente. Adesso molti sistemi usano: avatar AI che parlano voice AI chatbot conversazionali

Questo significa che quando l’utente scrive, la risposta non è più un messaggio automatico stupido, ma una conversazione abbastanza credibile.

In pratica sembra davvero una persona.

La truffa non è più immediata

Prima lo schema era semplice: video, sito, pagamento.

Adesso invece fanno così:

Reel seducente, Spostamento su Telegram / sito / chat privata, conversazione di qualche giorno creano un minimo di relazione. E solo dopo arrivano a chiedere soldi.

Questo è molto più efficace psicologicamente.

Il trucco più potente: il “video personalizzato”

Qui arriva la parte più interessante. Molte truffe ora usano video AI personalizzati.

Esempio: Tu scrivi *"Ciao"*. Dopo poco ricevi un video dove la ragazza dice: *"Ciao Claudio, grazie per avermi scritto."*

Ovviamente non è reale. È un avatar AI che genera il video automaticamente. Ma per chi non conosce queste tecnologie sembra una prova reale.

Il nuovo obiettivo: dati personali

Non sempre vogliono subito soldi.

Spesso cercano: numero di telefono, email, foto, documenti, accesso a piattaforme

Perché quei dati poi vengono usati per: altre truffe, ricatti, vendita nei database criminali.

Perché questo fenomeno esploderà

Per tre motivi:L'AI abbassa i costi: prima servivano modelle o foto rubate. Si possono creare migliaia di avatar. Gli algoritmi social amplificano i reel, quindi con pochissimo investimento possono raggiungere milioni di persone.

Da dove arrivare il guadagno economico ?

Il modello economico delle "ragazze AI"

Molti profili che vedi su Facebook, Instagram e TikTok sono gestiti come vere e proprie micro-aziende. L'obiettivo non è truffare subito qualcuno, ma portare traffico.

1. Reel virali

Pubblicano continuamente: video seducenti, avatar AI molto realistici, contenuti provocanti. Questo fa scattare l'algoritmo, con il risultato di milioni di visualizzazioni, utenti curiosi e commenti

2. Link esterni

Sotto ai video o nei messaggi automatici mettono link verso: siti di incontri, OnlyFans-like, chat premium, piattaforme di appuntamenti. Quando qualcuno si registra o paga qualcosa, l'account prende una commissione.

3. Guadagno a percentuale

Il sistema è quasi sempre affiliazione.

Esempio tipico:

- utente si iscrive → 10-20 € di commissione
- utente compra crediti chat → percentuale
- utente paga abbonamento → percentuale mensile

Se l'account porta centinaia di iscritti, i guadagni diventano molto alti.

4. Il trucco dell'AI

Con l'AI succede una cosa nuova: prima servivano modelle vere, foto, set fotografici. Adesso bastano: generatore di immagini, avatar video, chatbot

Con pochi strumenti si possono creare decine di "personaggi" diversi.

Perché i social non riescono a fermarlo

Perché tecnicamente: non è pornografia, non è una truffa evidente, spesso c'è scritto "sito di incontri" Quindi resta in quella zona grigia che le piattaforme fanno fatica a bloccare.

La vera novità è che una volta le truffe online richiedevano: call center, operatori, organizzazioni criminali. Oggi basta un computer e qualche software di AI. E puoi creare una donna che non esiste, che parla con migliaia di persone.

Come ricoscere una ragazza "AI"

Ecco i tre segnali semplici che spesso permettono di capire subito che dietro c'è una "ragazza AI" o un sistema automatico.

1. Il profilo è "troppo perfetto"

Quasi sempre il profilo ha: solo foto o video molto seducenti, nessuna foto normale (amici, famiglia, vita quotidiana), immagini tutte con lo stesso tipo di luce e stile.

Le persone vere pubblicano di tutto: vacanze, amici, momenti banali. Gli avatar AI invece sembrano usciti da uno studio fotografico permanente.

2. Risponde subito… a chiunque

Se commenti o metti un like, succede spesso questo: risposta immediata, messaggio molto generico, invito a spostarsi su un altro sito o una chat privata

Le frasi sono quasi sempre simili: *"Ho notato proprio te", "Preferisco parlare in privato", "Ti aspetto qui…"*

Questo significa quasi sempre messaggio automatico.

3. Vuole uscire dal social il prima possibile

Questo è il segnale più importante.

Ti chiedono subito di andare su: sito di incontri, Telegram, WhatsApp, link esterno.

Perché sui social sono controllati, mentre fuori possono fare quello che vogliono.

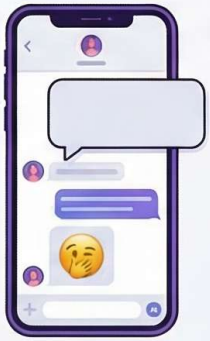
Attenzione alla “Ragazza Algoritmo”: Come Funzionano le Truffe AI sui Social

Le truffe online si sono evolute, non si usano più solo foto rubate, ma avatar AI realistici che parlano e interagiscono. Il processo mira a creare una falsa relazione psicologica per spingere l’utente a pagare servizi premium o cedere dati sensibili.

Il Ciclo della Truffa AI

L’Esca del Reel Virale

Video seducenti creati con AI per attirare visualizzazioni e commenti tramite algoritmi social.



Spostamento su Chat Private

Bot automatici invitano subito l’utente su Telegram o siti esterni per evitare controlli.

Telegram

Siti Esterni

La Manipolazione Economica

Richiesta di acquisto crediti, abbonamenti premium o furto di dati personali e documenti.

Come Riconoscere l’Avatar

Il Profilo “Troppo Perfetto”

Mancanza di foto di vita quotidiana, amici o ambienti reali; immagini stilisticamente identiche.

Reattività e Urgenza

Risposte istantanee e generiche che spingono costantemente a uscire dalla plattaforma social originale.

Video AI Personalizzati

L’avatar pronuncia il tuo nome nel video: sembra prova reale, ma è generazione automatica.

Confronto tra Truffe Tradizionali e Nuova Truffa AI

Caratteristica	Truffa Tradizionale	Nuova Truffa AI
Materiale Visivo	Foto rubate statiche	Video e avatar parianti
Interazione	Operatori umani o bet semplici	Chatbot conversasionali credibili
Costi per il Truffatore	Alti (personale/modelle)	Bassi (software AI scalabili)