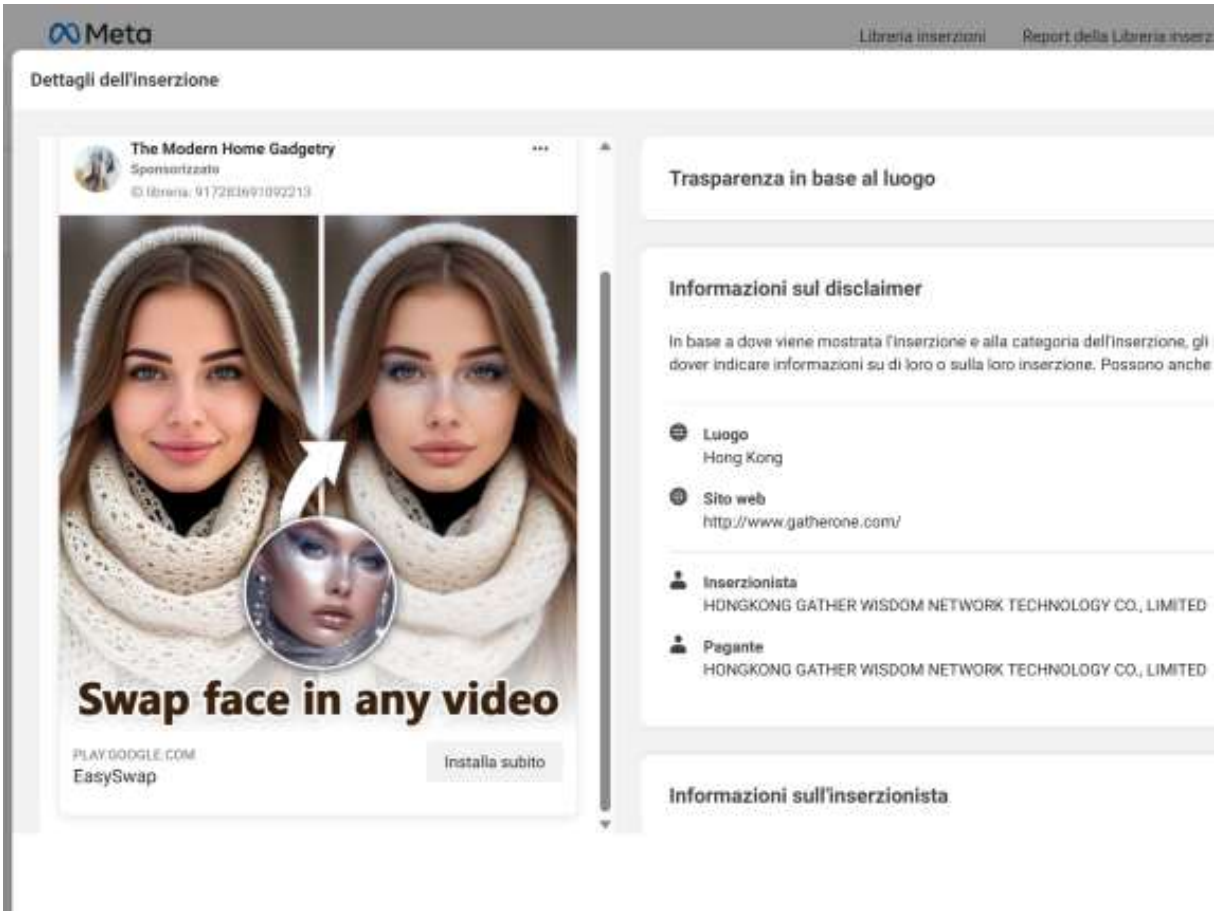
Come vengono distribuiti gli annunci truffa pubblicati su Facebook: la società cinese, l'app che ruba i profili, l'esca dei contenuti porno di Roberto Cosentino

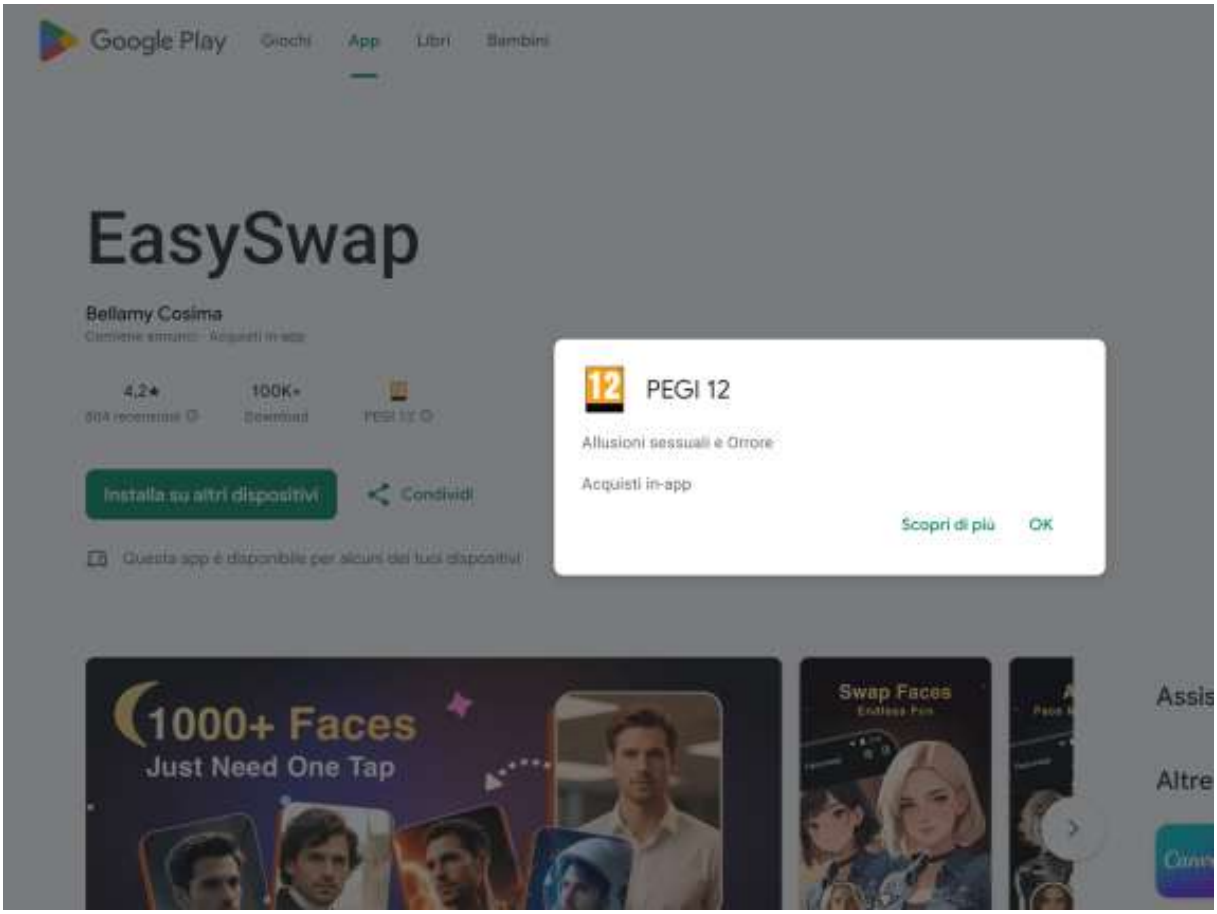
Uno schema complesso che smaschera come un'agenzia cinese partner di Meta riesca a pubblicare annunci truffaldini, sfrutti canali Telegram con revenge porn e rubi account per ritorni economici (Fonte: https://www.corriere.it/ 27 aprile 2026)



Meta ha da molto tempo un problema con le pubblicità. Negli ultimi tempi **ha implementato misure di sicurezza** che sfruttano l'intelligenza artificiale per filtrare gli annunci che promuovono truffe o altri contenuti illegali, ma non sempre si rivelano efficaci. Un'inchiesta di Reuters dello scorso inverno aveva rilevato come il 10 per cento degli introiti di Meta derivassero proprio dalla vendita degli spazi per i banner per sponsorizzare truffe ed estorsioni. Ma non è facile a risalire all'esatta dinamica con cui gli inserzionisti riescono a pubblicare tante pubblicità da account diversi. Abbiamo provato a seguire il percorso di una di queste aziende, partner di Meta, che ha sede in Cina. E ci siamo ritrovati a districarci tra **revenge porn, phishing e app per la creazione di deepnude.**

Tutto comincia da una pubblicità su Instagram

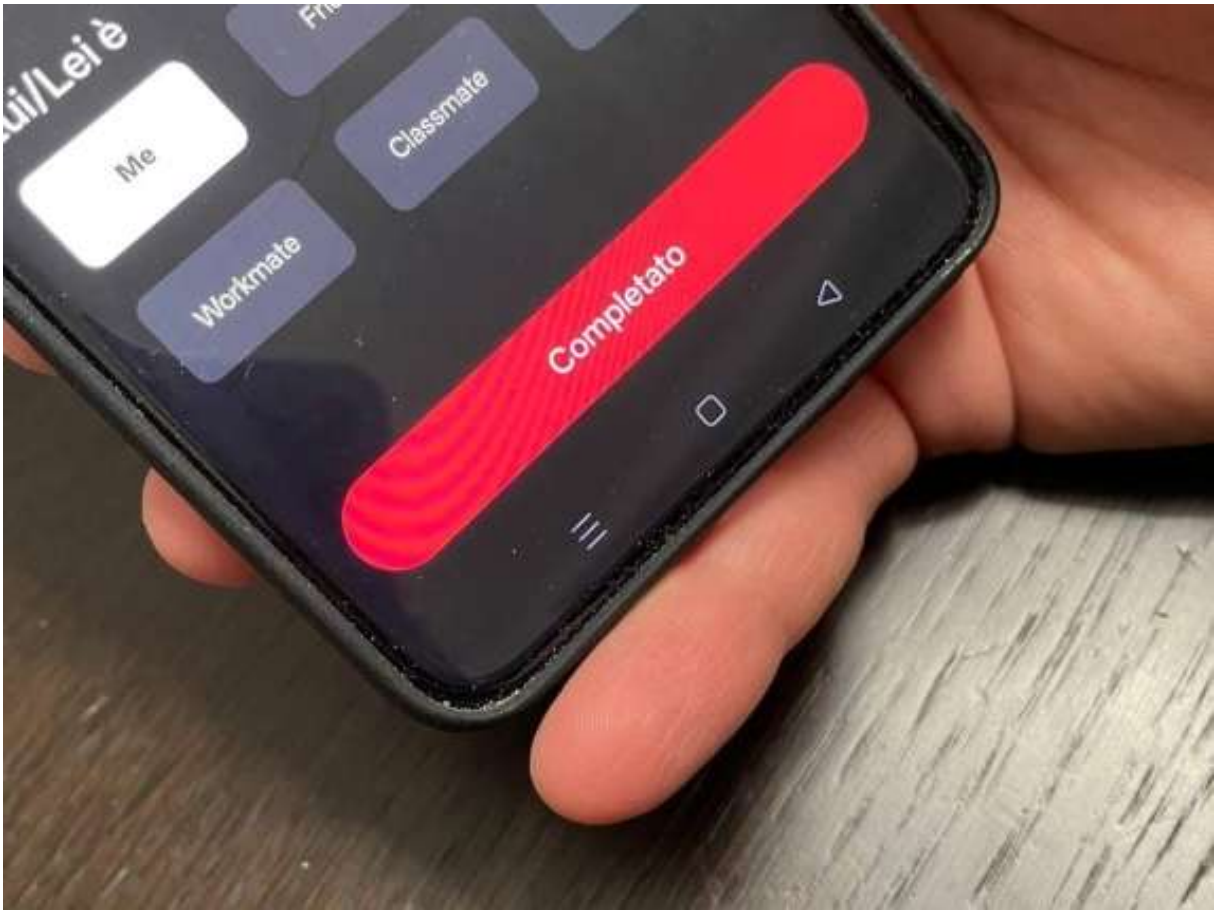
Non è la prima volta (e non sarà neanche l'ultima) che ci siamo imbattuti in una pubblicità sospetta che promuove un'app che promette la creazione di deepfake e deepnude. Una volta aperta, la prima schermata mostra contenuti di tipo pornografico. Un link ci porta poi a scaricare un'app dal Play Store: si chiama EasySwap ed è classificata Pegi 12.



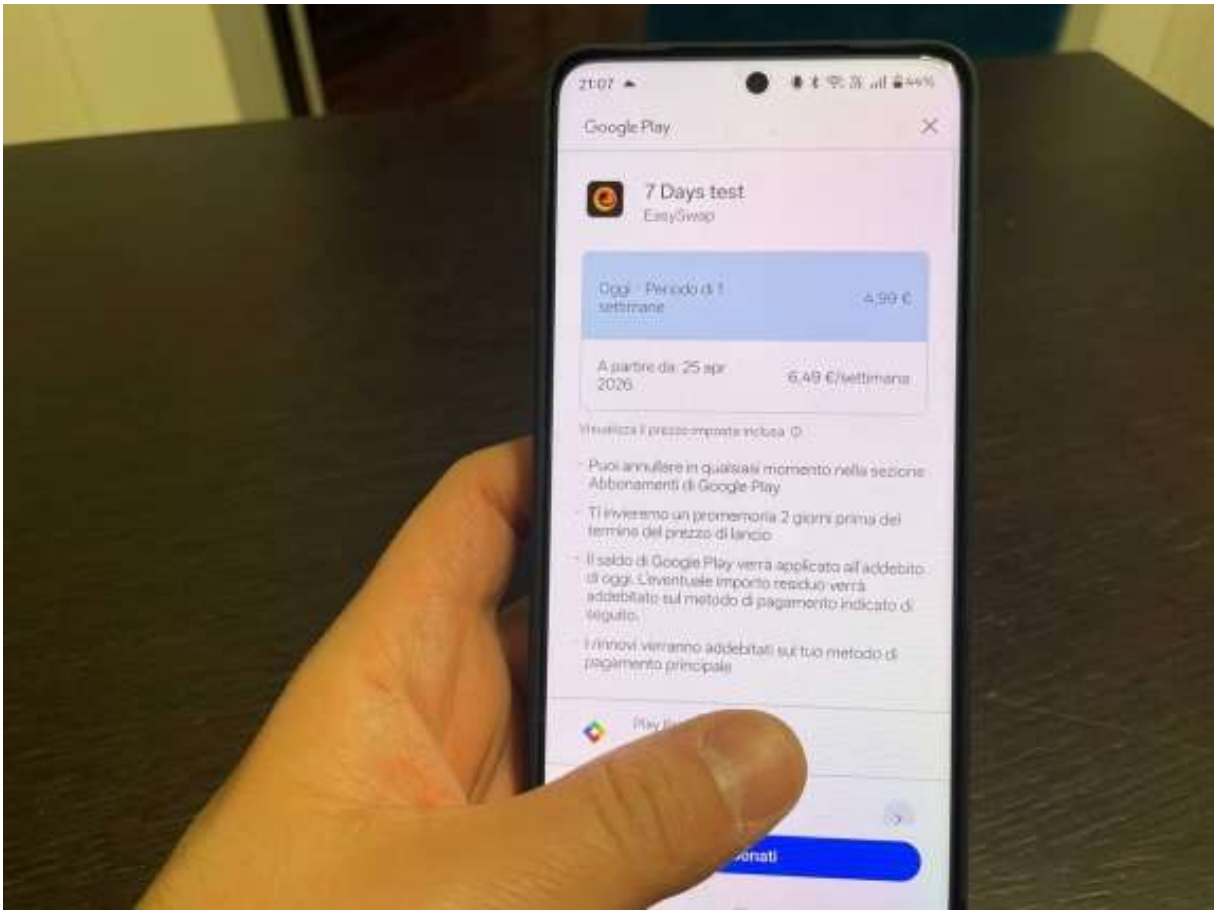
Pegi (Pan European Game Information) è il sistema europeo di classificazione dei videogiochi, che è stato introdotto più di 20 anni fa, per aiutare genitori e consumatori a scegliere prodotti che fossero adatti all'età dei minori. Classifica i giochi in 5 fasce d'età (3, 7, 12, 16, 18); in questo caso, **Pegi 12, avvisa che il contenuto è idoneo dai 12 anni a salire**, e la classificazione avvisa che vi è la possibilità di imbattersi in **allusioni sessuali** e contenuti horror. Horror non ne abbiamo visto, ma in compenso segnalare i contenuti mostrati come «allusione sessuale» è un vero eufemismo.

Come funziona l'app

La prima schermata dell'app, che **non consente di acquisire screenshot,** presenta delle gif pornografiche. Si può decidere di utilizzarli come base dei deepfake, ovvero modificare le sembianze delle attrici con quelle di altre persone. Per farlo, l'utente dovrà caricare le immagini sul proprio profilo. L'app consente di segnalare se le persone ritratte sono parenti, amici, compagni di classe.



L’app funziona a crediti o abbonamenti che in entrambi i casi si possono acquistare in prima istanza su **Play Store**. Le opzioni sono un pagamento a vita oppure un abbonamento mensile. Si può anche guadagnare crediti guardando pubblicità, oppure condividendo l’applicazione con amici.



Il revenge porn su Telegram

All'interno di questa app vi sono collegamenti ad una serie di gruppi affiliati a EasySwap. Uno di questi è su Telegram. All'interno di questo canale, gli utenti condividono prevalentemente foto di donne, loro conoscenti, e chiedono aiuto per la generazione di contenuti vietati ai minori, con le sembianze delle vittime. Uno dei bot presenti nel canale Telegram offre la possibilità di accedere ad altri tipi di contenuti, tra cui anche alcuni di **natura pedopornografica**. Il contenuto in realtà non esiste, ma cliccando sui pulsanti l'app rimanda ad un bot che utilizza un *escamotage* per far sì che l'utente consegni i propri dati per poi fargli perdere l'accesso al proprio account.

Una volta cliccato uno dei tasti, vengono avviate delle mini-app, pubblicate su **siti terzi** la cui provenienza è difficile da recuperare. Il loro scopo è **sottrarre il codice di accesso di Telegram** così da poter effettuare un "take-over" e cioè il controllo totale dell'account. E come vedremo tra poco, non succede solo con Telegram, ma anche con Facebook.

La schermata per sottrarre l'accesso

Chi c'è dietro a tutto questo

Consultando la library delle inserzioni di Meta correlate ad EasySwap sono associate alla società **HongKong Gather Wisdom Network Technology Co., Limited**. La compagnia è stata fondata nel 2015 e registrata nel 2016 ad Hong Kong e si occupa, stando a quanto affermato dalla stessa, di digital marketing / performance marketing. Più precisamente, la data di creazione risale al 7 gennaio 2016 e come indirizzo legale troviamo Room A, 29/F, United Centre, 95 Queensway, Admiralty, Hong Kong.

La società utilizza come alias il nome **GatherOne**. In diversi documenti viene attestata come **Facebook first-tier agent**, ovvero agente di primo livello di Facebook. Secondo un **documento finanziario** di una terza agenzia cinese che nulla c'entra con questa storia, è riportato che GatherOne **avrebbe subito condizioni di pagamento più rigide da parte di Facebook**, con conseguente maggiore **pressione finanziaria** e ritardi negli incassi. Il report su cui siamo riusciti a mettere mano non dipinge quella che può sembrare una semplice agenzia creativa, **ma un nodo di intermediazione adtech rilevante**.

Jayne Leung (a destra), Presidente di Meta Greater China

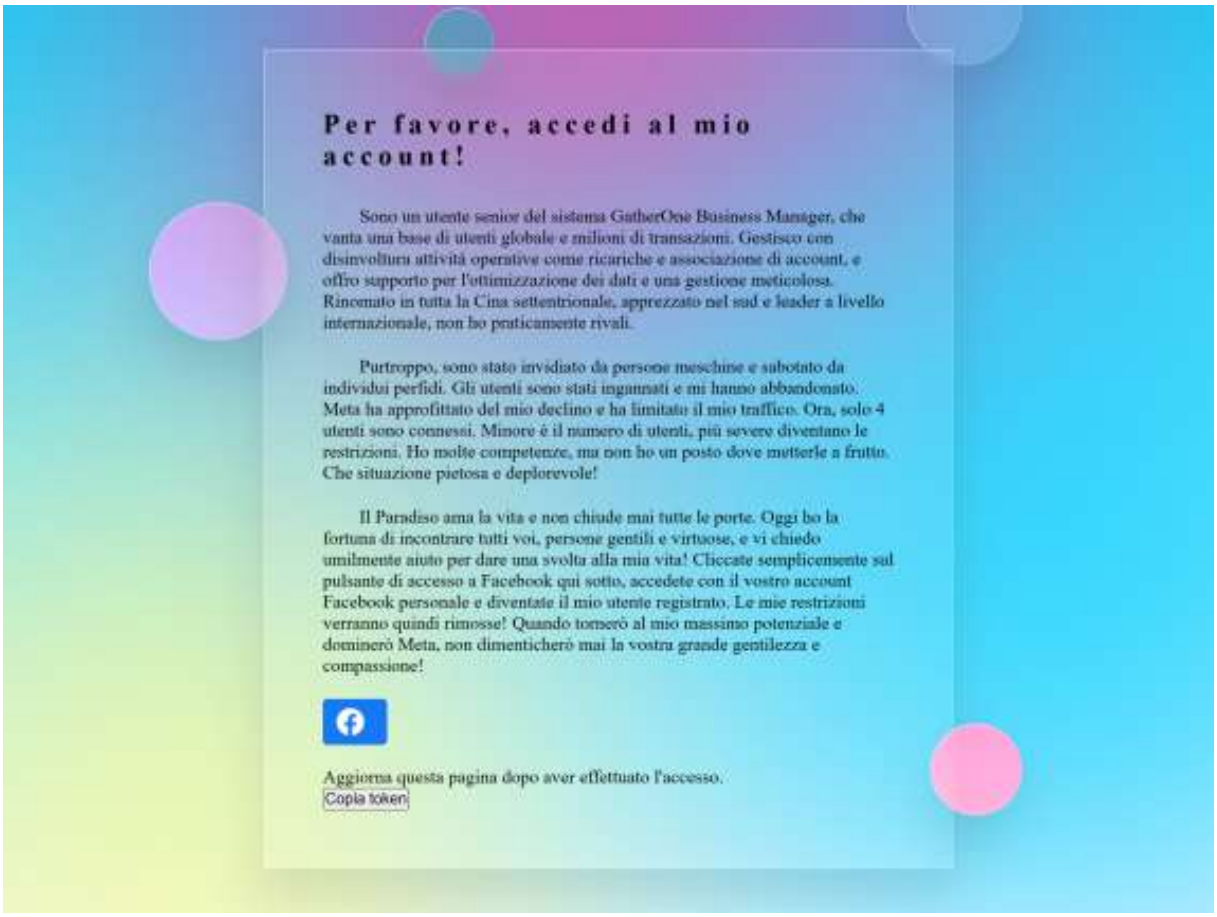
Andrew Wong (a sinistra), Direttore Generale del Canale Commerciale di Meta Greater China

Wang Hao (al centro), co-fondatore e CEO di GatherOne

In un post del blog del nuovo sito della compagnia, si legge:
«Da quando GatherOne è diventata ufficialmente distributore di primo livello di Meta nel 2019, le due parti hanno sviluppato un modello di cooperazione completo, dall'integrazione tecnologica e la condivisione delle risorse alla collaborazione sui servizi, e hanno assistito e partecipato insieme all'ascesa e allo sviluppo dell'ondata di marchi cinesi che si stanno globalizzando».
E ancora:
«Da quando hanno unito le forze, GatherOne e Meta hanno assistito e promosso la globalizzazione dei marchi cinesi. In futuro, GatherOne continuerà a trasformare la tecnologia intelligente, la sinergia dell'ecosistema e la visione a lungo termine in un sistema di crescita affidabile, impegnandosi a diventare un partner di valore più professionale, sistematico e duraturo per i marchi cinesi nel loro percorso di espansione globale».
Della stessa società si era già occupata **Reuters** a dicembre del 2025. All'epoca l'agenzia di stampa non si era imbattuta in applicazioni di deepnude, ma di vere e proprie truffe e già allora *Reuters* descriveva GatherOne come «one of Meta's top Chinese partners». Non solo. Secondo l'inchiesta del quotidiano, **alcuni account usati per testare inserzioni truffaldine risultavano collegati a partner cinesi più grandi**, tra cui proprio GatherOne. La società non ha risposto alle richieste di commento dell'agenzia. Nel sito ufficiale, la compagnia riferisce di aver ottenuto per tre anni consecutivi **il riconoscimento** di **Google annual excellent partner / Google Premier Partner**.

La rete capillare su Facebook per gli account pubblicitari

Su GatherOne ci siamo imbattuti in una pagina che chiede l'accesso al proprio profilo Facebook. In questo caso lo scopo non è rubare i profili, ma accedere alle possibilità di inserire inserzioni a nome di chi si lascia convincere. Il motivo è molto semplice. Pubblicare truffe o contenuti che potrebbero essere dannosi, come la pubblicità all'app di cui abbiamo parlato nell'introduzione, potrebbe portare alla disattivazione del profilo ufficiale dell'agenzia. Ma avere un esercito di profili business alla propria mercé, ne mette al sicuro la diffusione.

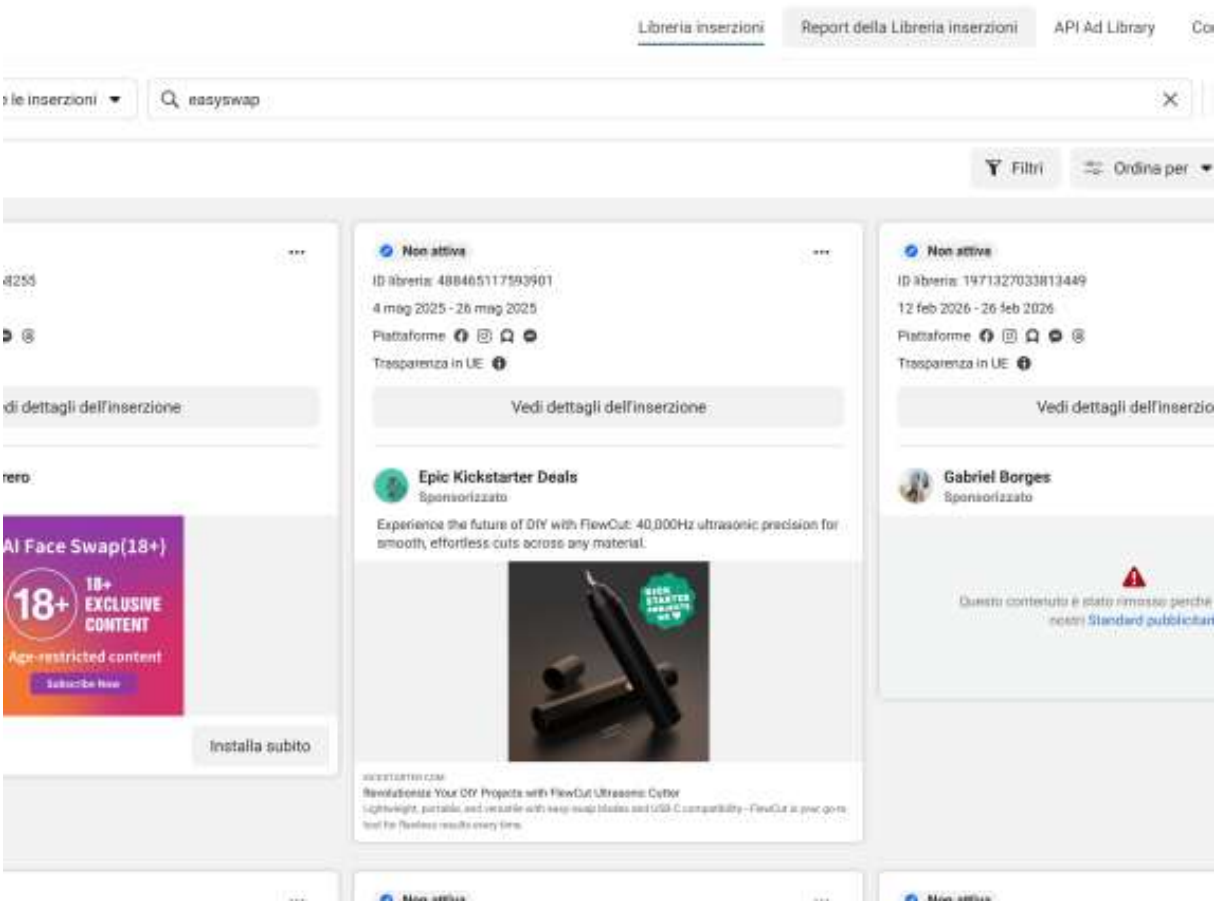


Andando ad ispezionare il codice **Html** della pagina, emerge una dinamica tanto interessante quanto inquietante. Il messaggio è in cinese, ma lo scopo è quello di ottenere da utenti reali un consenso per permessi business ad alto impatto. In particolare vengono richiesti (anzi, prelevati) i privilegi "**public_profile, email, ads_management, ads_read, read_insights, business_management**".

Come Meta documenta, ads_management consente a un'app di leggere e gestire account pubblicitari a cui l'utente ha accesso; ads_read serve per leggere dati e metriche pubblicitarie; read_insights permette di leggere dati di insight; business_management è il permesso usato per gestire asset e funzioni del business portfolio tramite le Business Management API. Non sono permessi da "login standard", ma da operatività su advertising e business assets. La base è sempre la stessa: un phishing avanzato con ingegneria sociale.

E questo spiega il motivo per cui la maggior parte delle inserzioni di app truffaldine o vietate ai minori siano pubblicizzate da pagine che sembrano totalmente al di fuori di qualsiasi schema di

pubblicità, ma pensate ad uso personale o amatoriale. Basta guardare l'immagine sottostante: **Cornelius Guerrero**, **Gabriel Borges**… Non sembrano nomi di un'agenzia partner di **Meta**. E questo non è un caso isolato. Basta fare delle semplici ricerche: le ads library di Meta sono pubbliche e accessibili a chiunque.



Tutto per i soldi

Lo schema è tanto contorto quanto geniale, pianificato da una piattaforma che ha accordi economici con le compagnie statunitensi perché a tutti gli attori coinvolti, arrivano soldi. **Peccato che a farne le spese, siano le persone comuni**. Le donne ancora una volta vedono violate la propria intimità, anche digitale, e si trovano **protagoniste involontarie** di video e immagini in cui i loro corpi sono alla mercé di uomini senza dignità né scrupoli. Dall'altra parte, i proprietari legittimi dei propri account, per perpetrare quelle che sono vere e proprie violenze digitali, si vedono **invece derubati dei loro account privati**. In attesa di capire se si troverà un modo di bandire pratiche di questo tipo da spazi digitali abitati da tutti noi - minori compresi - abbiamo segnalato tutto ciò che vi abbiamo raccontato alla Polizia Postale.