CyberArmor

'25

Meta Phishing Operations

Targeting Business Accounts

DATE

Nov 20, 2025

AUTHORS

Veronika Katsevych

Table of Contents

Executive Summary

CyberArmor Threat Intelligence has uncovered a coordinated phishing campaign targeting Meta Business Manager and Ads Manager accounts globally. Over the past year, more than 20,916 credentials were submitted to attacker-controlled systems. The activity is deliberate, structured, and engineered to exploit user trust.

Victims receive messages formatted as official Meta alerts, referencing policy issues, copyright disputes, or account suspensions. The communication appears urgent, credible, and professionally crafted.

After obtaining credentials, attackers act quickly by:

- Removing authorized administrators
- Modifying payment methods
- Launching fraudulent advertising campaigns
- Depleting advertising balances
- Harming brand integrity

The full compromise sequence can occur in less than ten minutes.

This report details the attack lifecycle, identifies the operators involved, and offers practical mitigation guidance.

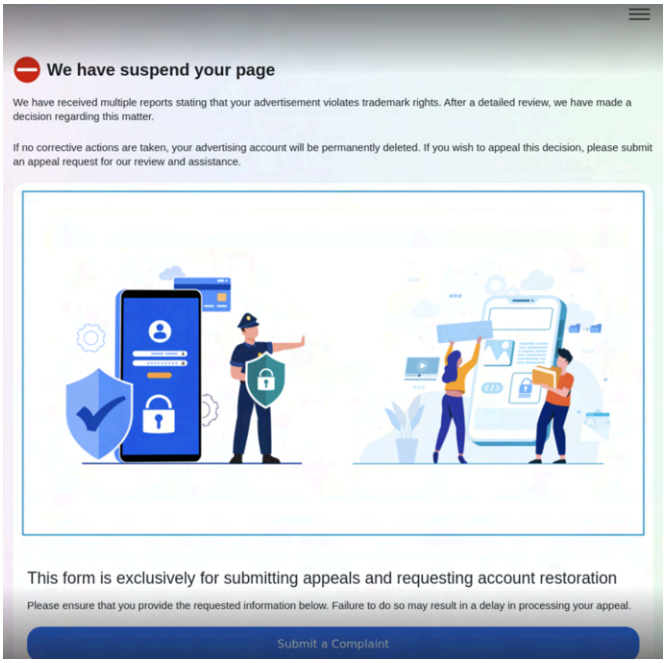
How Cybercriminal Perform The Attacks

Phishing Attacks

The attack starts with a message crafted to create urgency and concern. These messages mimic Meta's branding and communication style, warning the recipient of policy violations, intellectual property issues, or unusual activity. Each message includes a button such as "Appeal," "Verify," or "Resolve Problem," which directs the user to a fraudulent Meta login page operated by the attackers.

Policy Violation Example

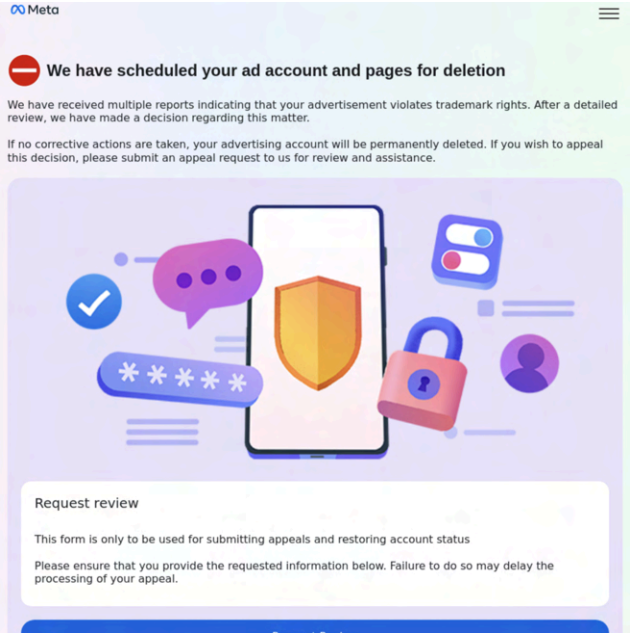
As shown in the following image, one variant of the phishing email uses a policy-violation theme, informing the user that automated activity was detected on the account. The message maintains a professional tone and concludes with a prompt to "resolve the problem."



Example phishing email using "policy violation" lure to trick Meta advertisers into verification.

Trademark Rights Example

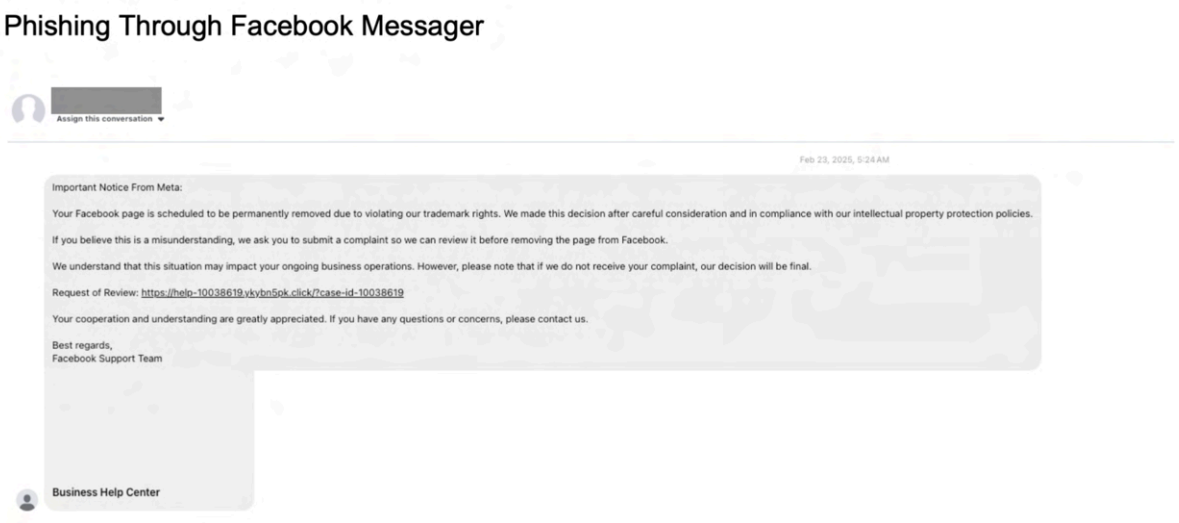
The screenshot below shows a phishing page impersonating Meta and claiming the user's ad account is scheduled for deletion due to trademark violations. The page uses a polished layout, complete with a shield graphic and soft visual elements, to reinforce credibility while steering the victim toward an appeal form. The wording urges swift action, matching the sense of urgency attackers rely on to push users forward without confirming authenticity.



Replica of Meta's "appeal" page

Example of a phishing email

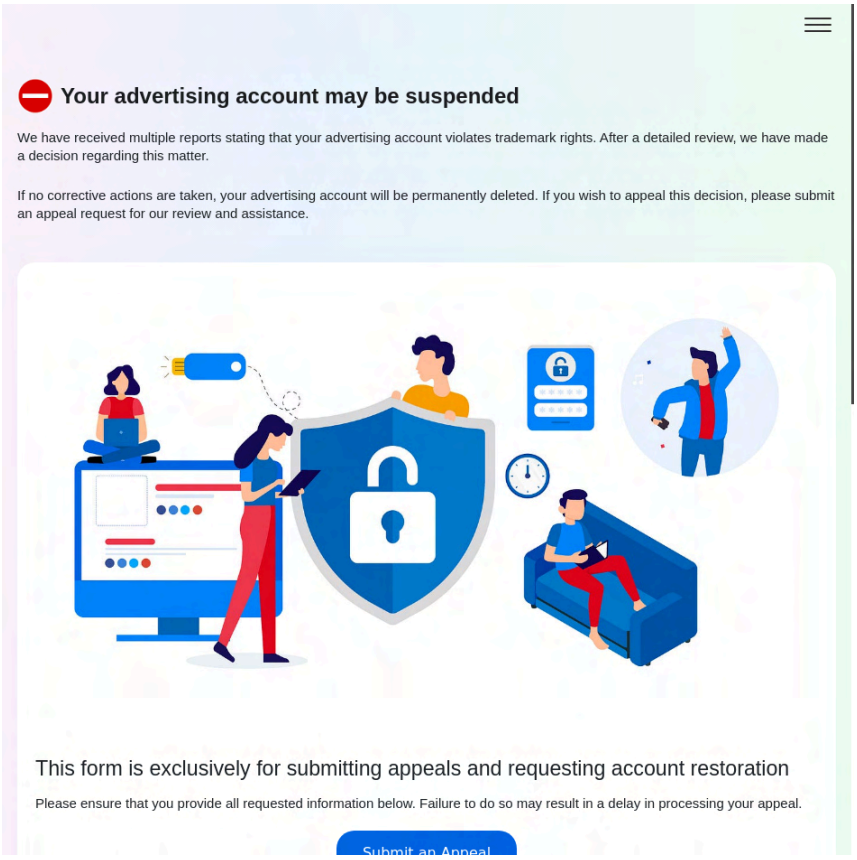
The message claims that the user's Facebook page will be permanently removed for violating "trademark rights." It's written in a tone that mimics the way Meta communicates official policy updates. The email includes a link for "reviewing" or "appealing" the decision, which actually leads to a phishing page designed to steal login credentials.



Message sent through Facebook Messenger, using a "trademark rights" violation lure to pressure victims into clicking a fake Meta link.

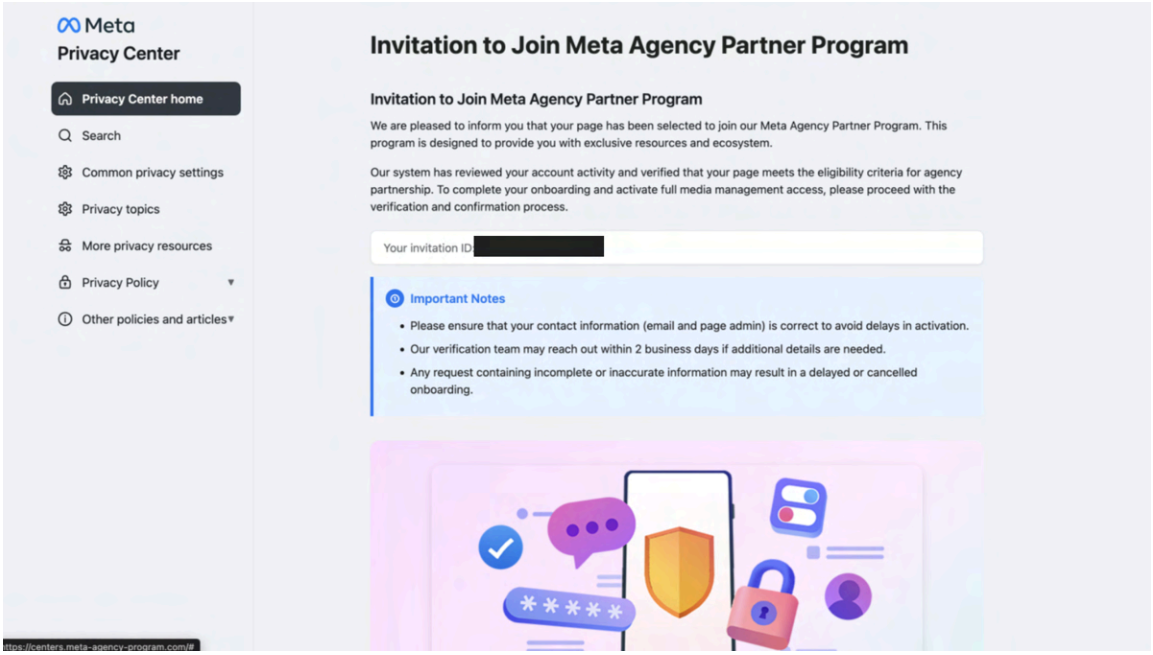
Phishing Webpage

Once the user clicks the link in the email, they are taken to a phishing site designed to capture their credentials. The page mirrors the theme of the phishing email, claiming the account is suspended and prompting the user to enter their username and password to restore access. Below are screenshots of the phishing pages.

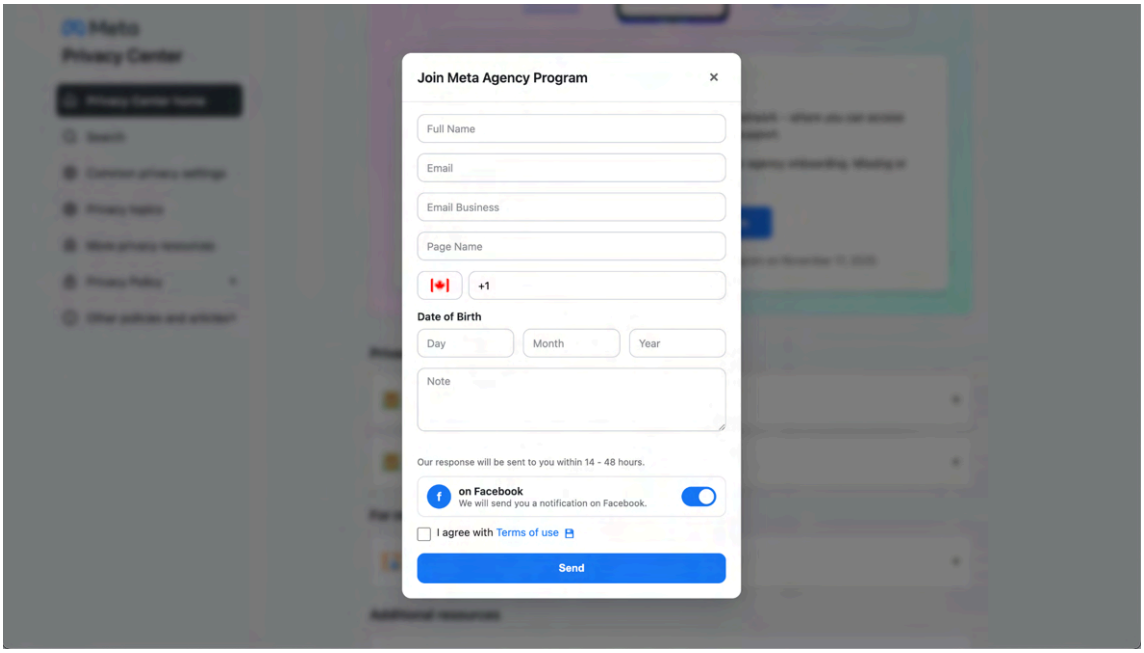


Trademark Violation Phishing Page

In addition to the violation theme, we also observed phishing attacks leveraging Meta's Agency Partner Program to deceive users into providing their information. Below are recent examples of phishing pages impersonating the Agency Partner Program.



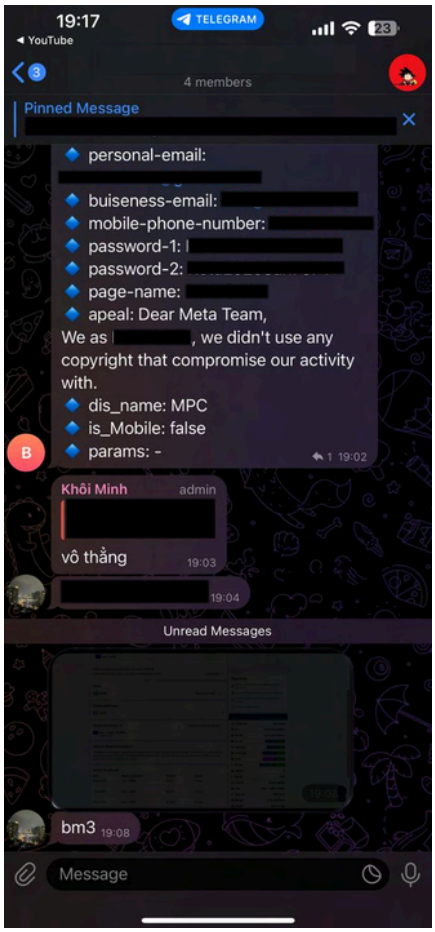
Fake Meta Agency Partner Program Page



Fake Meta Agency Onboarding Form

Stolen Credentials

Once the victim enters their credentials and submits the phishing form, the cybercriminals receive the data in near real time through Telegram. As shown in the image below, the chat contains the credentials submitted by a victim. The image also shows the operators working as a group, logging into the victim's account and sharing a screenshot as proof. The conversation, written in Vietnamese, includes a comment noting successful access, indicating that the account did not have two-factor authentication enabled.



Redacted chat logs showing actors confirming successful account access and discussing 2FA bypass.

Bypassing Two-Factor Authentication

Attackers do not bypass 2FA; they intercept it. When victims enter their one-time code into the phishing page, the code is forwarded to the attacker immediately, allowing them to log in before it expires. Once inside, the attacker marks the device as trusted or adjusts security settings to block the account owner from regaining access. This method works against SMS and app-based 2FA but not against hardware security keys.

The image below shows a login challenge screen with a failed two-factor authentication attempt. The page instructs the user to open their authentication app, such as Duo Mobile or Google Authenticator, to retrieve a six-digit verification code. A code has been entered but rejected, indicated by a red validation message beneath the field. The layout features an illustration of a hand tapping a phone, along with buttons to continue or choose an alternative verification method. The design closely imitates Meta's legitimate verification interface, enhancing its credibility.

Failed 2FA entry screen mimicking Meta's verification process

Why Does The Attack Work?

The attackers operate with discipline and consistency. Their internal chat logs show collaboration, debugging, testing, and template updates throughout the day. They behave like a functioning technical team, not casual cybercriminals.

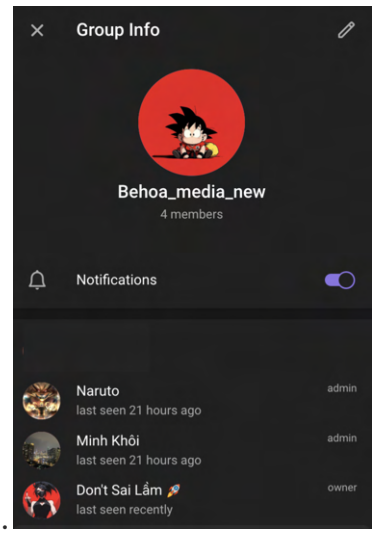
On the victim side, the attack succeeds because it exploits trust, urgency, and the fear of losing business visibility. When a message appears to come from Meta and threatens suspension, many users click without verifying the source. This human response is the central weakness the attackers rely on.

Who Are These Cybercriminals

Vietnamese-Based Operator Group

Evidence strongly suggests the campaign is operated by a small but highly coordinated group based in Vietnam. Their activity patterns align with Vietnamese business hours, their dashboards and internal chatter include Vietnamese language, and their payment trails connect to services commonly used within the region.

The image below shows a Telegram group used by the operators behind this phishing and ad-hijacking activity. The membership list confirms that this is a small, focused Vietnamese team working together in a coordinated way. The group includes one primary controller, two members who appear responsible for managing ongoing operations, and an additional participant who likely assists with testing and day-to-day tasks. The structure reflects a streamlined setup typical of small threat groups that operate efficiently, communicate frequently, and execute their workflow with clear role separation.



Screenshot of a private messaging group

Motivation

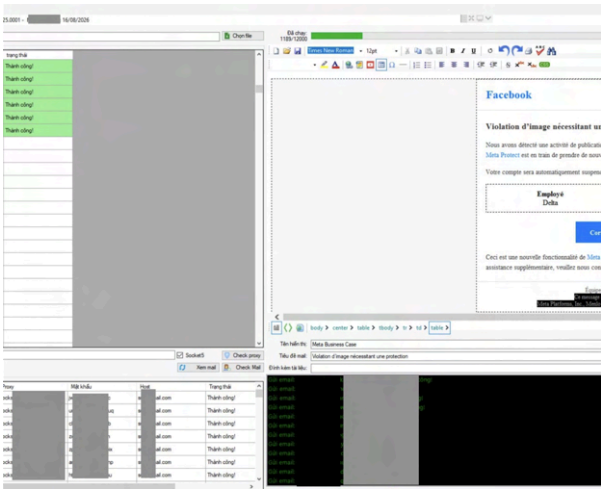
The operation is financially driven. Stolen credentials are immediately used to take control of Meta ad accounts, attach payment methods, and run fraudulent advertising campaigns designed to generate revenue as quickly as possible. There is no indication of political or espionage motives.

Target

The campaign targets individuals who manage business assets on Meta - advertisers, digital marketers, and business owners. These accounts are valuable because they contain active payment methods, advertising budgets, and administrative privileges. Attackers select victims based on publicly visible signals such as verified pages, active ads, sponsored posts, and high engagement. Small and mid-sized businesses are especially vulnerable due to limited cybersecurity resources and the multitasking nature of their operations.

Phishing Email Campaign

The image below provides insight into how these cybercriminals operate. The operator can craft phishing messages and distribute them to hundreds of users. The interface includes template editors, delivery status indicators, and proxy management features, illustrating how attackers industrialize their operations. Each outbound email is automatically logged, reflecting a streamlined system for sending large volumes of impersonated Meta notifications.

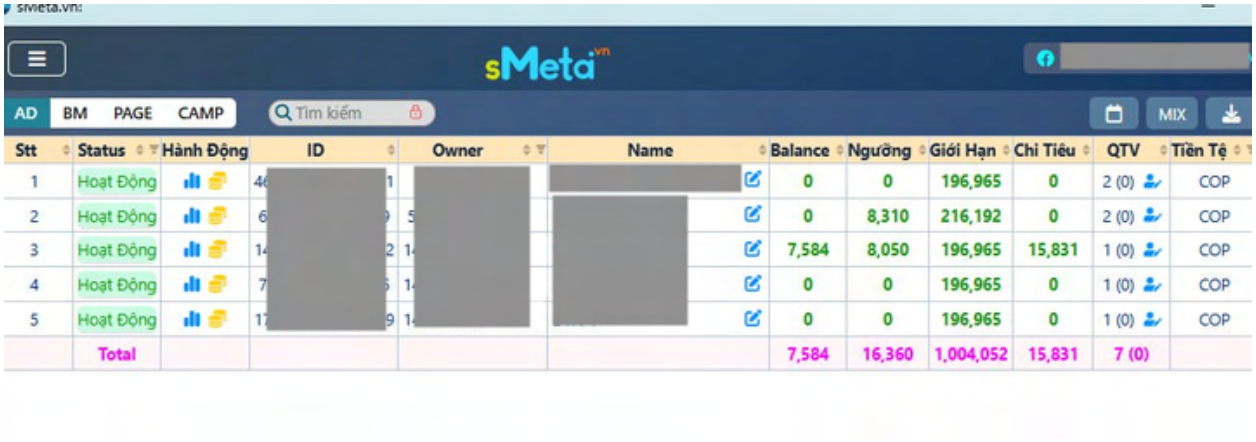


Backend panel used by attackers to send bulk phishing messages. The tool automatically fills in victim data and sends emails at scale.

Attacker’s control panel

The image below shows a Vietnamese attacker’s control panel (sMeta.vn) used to manage multiple compromised Meta advertising accounts. Each row represents a hijacked account, displaying key financial details such as balance, spending limit, and currency(in this case, Colombian Pesos – COP).

All accounts are marked as “Hoạt Động” (Active), indicating that they are still being used for fraudulent ad activity. The totals at the bottom summarize combined available funds and ad limits across all stolen accounts, showing how the attackers systematically monitor and exploit victims’ ad budgets through one centralized management system.



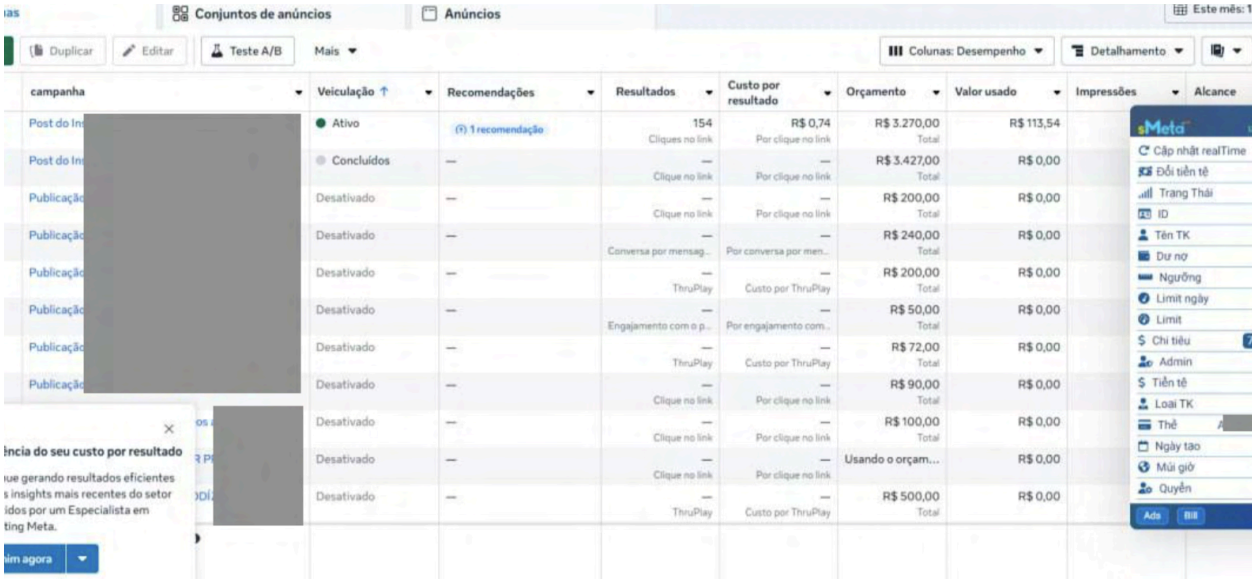
Stt	Status	Hành Động	ID	Owner	Name	Balance	Ngưỡng	Giới Hạn	Chi Tiêu	QTV	Tiền Tệ
1	Hoạt Động		[redacted]	[redacted]	[redacted]	0	0	196,965	0	2 (0)	COP
2	Hoạt Động		[redacted]			0	8,310	216,192	0	2 (0)	COP
3	Hoạt Động		[redacted]			7,584	8,050	196,965	15,831	1 (0)	COP
4	Hoạt Động		[redacted]			0	0	196,965	0	1 (0)	COP
5	Hoạt Động		[redacted]			0	0	196,965	0	1 (0)	COP
	Total					7,584	16,360	1,004,052	15,831	7 (0)	

The dashboard displays each victim's account and associated advertising balance

This screenshot below shows a compromised Brazilian Meta Ads account actively running fraudulent campaigns while the attacker's sMeta.vn control panel is open on the right side.

On the left, several ads are marked as active or recently completed. On the right, the attacker's dashboard displays the hijacked account's ID, card type, time zone, admin role, and real-time spending limits.

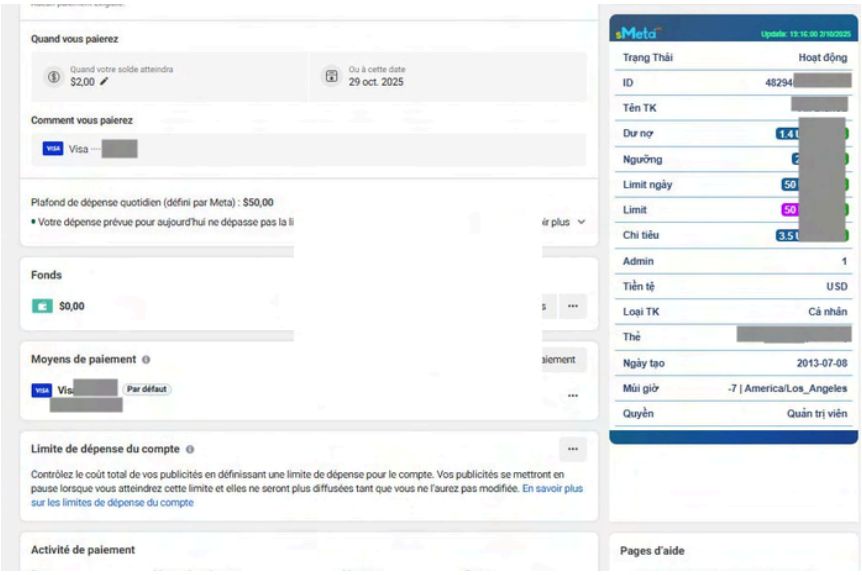
This dual interface confirms that scammers were running large-scale ad campaigns at the exact moment the victim still had access to their Ads Manager, highlighting how quickly stolen accounts are monetized once credentials are captured



Message flow visualization showing interconnected phishing templates and operator nodes

The screenshot below provides clear evidence of an active account takeover. While the victim continues to view their billing information normally within Meta's interface, the attackers are simultaneously observing the same details through their custom sMeta control panel. This real-time mirroring confirms that the victim's credentials have already been stolen and that the attackers have successfully logged into the account.

By monitoring available balances, limits, and payment activity, the operators evaluate how much they can spend on fraudulent advertisements before the victim notices. This side-by-side visibility demonstrates how quickly stolen credentials transition from simple capture to immediate weaponization, connecting the phishing phase directly to the financial exploitation that follows. The accompanying credential-capture interface, which imitates Meta's business login page, illustrates the level of detail used to deceive victims, with sensitive fields redacted for security.



Interface imitating Meta's business login form

This is where the damage multiplies. Not only does the business lose control, but its reputation also suffers when customers see scam ads under its name.

This issue reflects a much larger trend across Meta's ecosystem. According to a recent Reuters investigation (November 2025), internal company documents showed that roughly 10% of Meta's 2024 ad revenue around US $16 billion may have originated from fraudulent or policy-violating ads.

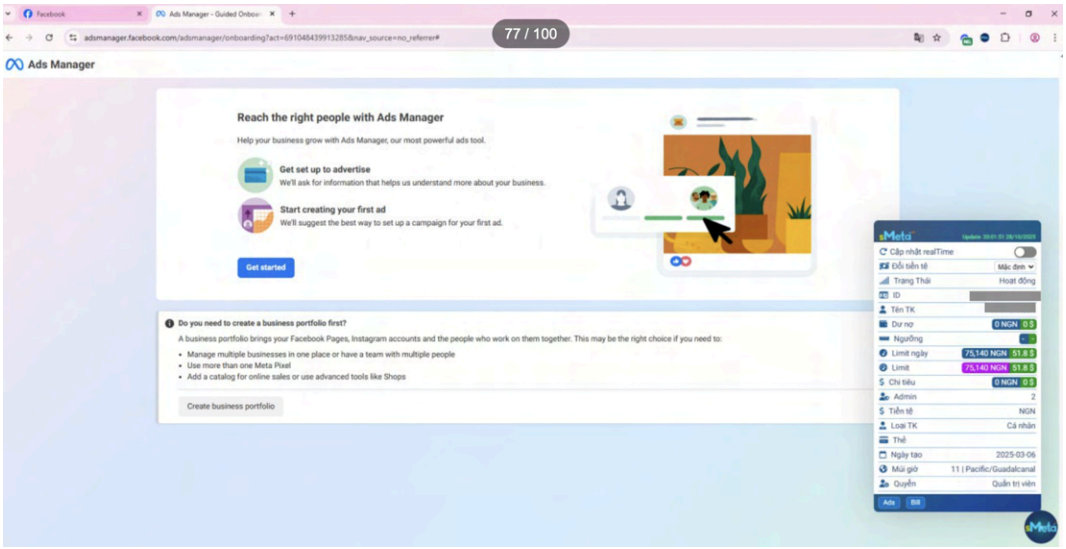
The report estimated that users were exposed to as many as 15 billion "high-risk" scam ads per day, underscoring how large-scale abuse of Meta's advertising infrastructure continues to generate massive financial impact both for victims and for the platform itself.

These findings highlight how the phishing operations we investigated fit into a wider, monetization-driven ecosystem - one where criminal actors exploit the same systems that legitimate advertisers rely on.

Evidence of Active Takeover

This screenshot shows a fake Meta Ads Manager page being accessed while a Vietnamese attacker control panel (sMeta.vn) is open on the right.The Meta Ads interface looks legitimate and invites the user to “Get started” - but the sMeta panel reveals the real purpose: tracking a compromised advertising account in real time.
The sMeta dashboard shows the victim’s account ID, currency (Nigerian Naira – NGN), spending limits, and admin permissions - confirming that the attackers have already taken control.

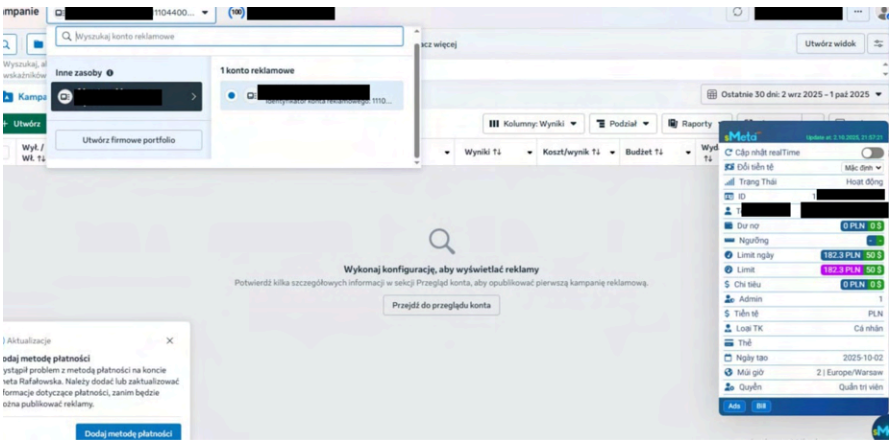
This setup illustrates how Vietnamese operators monitor hijacked Meta accounts through their own tools, often using them to run scam ads or drain advertising balances within minutes of gaining access.



Redacted screenshot of a compromised Meta Ads Manager session, showing attacker-linked management panels and altered payment settings.

Payment Manipulation Attempts

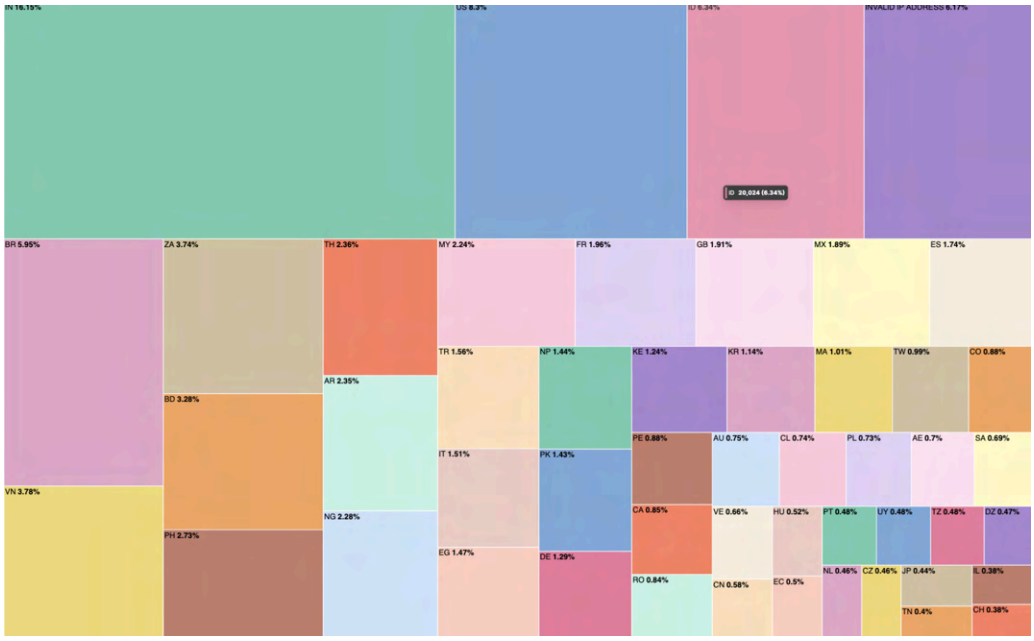
Once the attackers take over an account, they can modify its settings, including ad campaigns and payment information. The example below shows a compromised account where the attackers are reviewing the payment history.



Example of a hijacked ad account showing altered billing configuration and spending limits.

Global Distribution

The campaign affected users in over forty countries, with no specific region, industry, or language targeted. Attackers used automated translation tools to adapt phishing pages into local languages, enabling successful targeting in the United States, India, Italy, Germany, Brazil, France, Indonesia, and many others. A heatmap of affected accounts shows the highest concentrations of victims in North America and Western Europe.



Global Victim Heatmap

A treemap analysis further highlights country-specific victim percentages, with India, the United States, and Indonesia representing the largest clusters identified.

Treemap of Victim Distribution

The geographic breadth of the attacks demonstrates how localization and automation have allowed a small team to operate globally without maintaining dedicated regional branches or language specialists.

How to Protect Yourself

Even without technical indicators, several behavioral signs help identify these attacks. Messages always contain urgency or a deadline, and while they mimic Meta's voice, certain phrases are subtly incorrect. Links rarely lead to official Meta domains, and fake help pages ask for sensitive information no legitimate platform would request through an appeal process. After compromise, unexpected ads, payment alerts, or new administrator roles appear within minutes.

1. Don't trust urgent messages

   If you get a message saying your Facebook or Instagram account will be "disabled" or "deleted" stay calm. Meta doesn't send suspension warnings through Messenger, WhatsApp, or email links.

2. Check the link before you click

   Real Meta links start with facebook.com or meta.com.
   If you see anything strange, extra words, numbers, or misspellings don't open it. If you're not sure, log in directly through the Facebook app or website instead of clicking the link.

3. Sign in safely

   Go directly to business.facebook.com or facebook.com - never through links in messages. Always type the address yourself.

4. Protect your login

   Turn on two-factor authentication (2FA) and use a security key if possible. Never share your 2FA code on any website or with anyone who messages you.

5. Watch for strange account activity

   If you notice new ads, payments, or login alerts you don't recognize, change your password immediately and review your security settings.

6. Be cautious with “support” offers

   No real Meta employee will contact you through Telegram, Messenger, or Instagram DMs to fix your account - those are scammers.

MITRE ATT&CK (High-Level Mapping)

MITRE ATT&CK is a global framework that categorizes real-world attacker behaviors into defined tactics and techniques, helping analysts understand and map each stage of an intrusion.

- **Initial Access:** Phishing – *T1566*
  Attackers send fake Meta “policy violation” messages to lure victims into clicking malicious links.
- **Credential Access:** Input Capture via Web Forms – *T1056*
  Victims enter their login details on cloned Meta pages controlled by the attackers.
- **Discovery:** Gather Victim Identity Information – *T1589*
  Collected credentials are used to identify ad account owners, payment methods, and linked business assets.
- **Defense Evasion:** Obfuscated HTML/JavaScript – *T1027*
  Phishing pages use encoded or hidden scripts to bypass detection and hide malicious code.
- **Command & Control:** Web Protocols / Services – *T1071, T1102*
  Stolen data is sent to Telegram bots and remote web servers over HTTPS.
- **Impact:** Business Process Abuse (ads, billing)
  Attackers exploit compromised ad accounts to run fraudulent ad campaigns and steal funds.

Conclusion

The Meta phishing campaign demonstrates how cybercrime has shifted from technical exploits to large-scale behavioral manipulation. Its effectiveness lies not in sophisticated technology, but in understanding human behavior - how business owners think, how urgency influences decisions, and how trust in familiar brands can be exploited.

The attackers operate with speed, discipline, and intent, using a repeatable model that combines marketing psychology, automation, and social engineering to target digital advertising systems worldwide. This underscores a key reality: modern phishing is less about hacking systems and more about manipulating workflows.

For organizations, traditional defenses alone are insufficient. Firewalls and antivirus software cannot prevent users from responding to convincing messages. Effective defense requires a combination of secure technology and vigilant personnel: using strong authentication that phishing cannot bypass, enforcing verification steps before approving changes or payments, and training teams to pause and verify before acting on urgent messages. At CyberArmor, we help organizations cultivate these practices so people and systems together can intercept attacks early.

As businesses increasingly rely on platforms like Meta, the human factor remains both the greatest vulnerability and the strongest defense. Building resilience requires awareness-empowering every employee to recognize when trust is being exploited against them.