Watchdog Finds Flourishing Black Market on Facebook for Fraudulent Ad Accounts

John P. Mello Jr.

November 15, 2022

A technology platform watchdog group reported Monday that it had found more than 100 Facebook groups, some with tens of thousands of members, where business management accounts are bought and sold in violation of the social network's rules.

The accounts can be used to run multiple pages and ad campaigns, creating new opportunities for online scams, disinformation, and election interference, according to the investigation by the Tech Transparency Project, a Washington, D.C.-based information and research organization that focuses on the influence of major technology platforms on society.

"For years, Facebook has claimed that its artificial intelligence systems can clean up its platform, but time and time again, we have found that Facebook's technology is failing to remove harmful content that violates its policies," the TTP's director Katie Paul told TechNewsWorld. "This is unfortunately true for this black market for ad accounts as well."

The TTP explained that business manager accounts allow social media managers and marketers to manage a collection of Facebook ad accounts, Facebook pages, and Instagram accounts from one dashboard. It added that Facebook's parent company Meta promotes them as a "one-stop shop" for advertising and marketing on its platforms.

The report contended that the accounts are particularly valuable to scammers because business managers can run a series of ad campaigns and easily add new users and ad accounts to expand their reach.

In the Facebook groups examined by TTP, the group noted that users frequently sell accounts in bulk quantities. Many of the accounts come linked to someone's credit card, it continued, indicating they were hacked or stolen. "That's obviously a big problem for individual users or small businesses that suddenly have an unauthorized person racking up big charges on their card," Paul said.

The report also found that in some cases, sellers offer accounts approved to advertise political, election, and social issues.

Facebook Acts

After being alerted to the situation, Facebook began dismantling the black market. “We removed the groups that were flagged to us last week for violating our policies, and we will continue to review additional groups and remove those that violate.” the company said in a statement provided to TechNewsWorld by spokesperson Erin McPike.

In addition to removing the groups, the company said it has set up checkpoints for several group administrators, requiring additional information to be provided before they can access their accounts.

Despite Facebook’s actions, the report maintains that the black market raises some troubling questions for the company and its parent, Meta. Given Facebook’s longstanding scam ad problem and its history with Russian election interference, it’s not clear why Meta isn’t doing more to combat this illicit trade, the report noted.

Jenny Griesdorn, senior manager of global social media strategy at KnowBe4, a security awareness training provider in Clearwater, Fla., cited Facebook’s community guidelines as evidence of its lack of concern about fraudulent accounts. Those guidelines state, “We may disable or delete your account if it appears to have been hacked or compromised and we are unable to confirm ownership of the account after a year.”

“That should be enough of a tell that Facebook does not care about getting rid of these fake or hacked accounts, so it’s best that anyone who uses this platform protect their personal information as much as possible,” Griesdorn told TechNewsWorld.

Fake Accounts, Real Revenue

Some critics of Facebook have suggested that the social network has taken a light touch to fraudulent accounts because they produce revenue.

“These black-market business manager accounts are approved to advertise on Facebook. That means that Facebook profits every time the buyers of these illicit accounts run ads on the platform,” Paul said.

“This raises new questions about how much of Facebook’s advertising revenue is coming from hacked, stolen, or trafficked ad accounts,” she added.

While acknowledging that Facebook can make money off fraudulent accounts, Will Duffield, a policy analyst with the Cato Institute, a Washington, D.C. think tank, pointed out that fake accounts don’t produce as much revenue as legitimate ones.

“There’s some incentive not to poke too much at the problem, but from the business side, each black market account means there’s a business customer who is dissatisfied because they’ve had their account stolen,” Duffield told TechNewsWorld.

“If legitimate accounts are being stolen and turned into black market accounts, that’s not good for Facebook,” he said.

Platform for Election Interference

According to the TTP report, Facebook has had a longstanding problem with accounts being hijacked to run scam ads using people's credit card information. It's easy to see how business manager accounts could be useful to scammers, the report continued, given their ability to run multiple ad campaigns simultaneously.

It added that owners of business manager accounts have frequently recounted how hackers commandeered their accounts, raising their billing threshold to rack up thousands of dollars in spending on scam ads that direct people to questionable e-commerce websites.

The TTP's investigation also found sellers offering accounts that can run ads on social issues, elections, or politics. That raises concerns they could be used for coordinated inauthentic activity and election interference, the report noted.

"Facebook executives often tout their efforts to curb election interference, but at the same time, the company is facilitating a black market for accounts that can run election ads in specific countries," Paul said.

"Facebook is essentially undermining its own election protection efforts with its failure to address this issue," she continued. "The Facebook business manager accounts identified by TTP are especially concerning because they can run multiple ad campaigns simultaneously, increasing the ability of bad actors to spread disinformation."

Challenging Task

Controlling disinformation on Facebook is a challenging problem, maintained Vincent Raynauld, an associate professor in the Department of Communication Studies at Emerson College in Boston.

"Identifying and suppressing disinformation is extremely hard for Facebook because the manifestation of disinformation on these platforms keeps evolving," Raynauld told TechNewsWorld.

"If Facebook establishes a filter to catch certain kinds of disinformation, the producers of the disinformation will adjust the structure of it so it will evade the filter and have an impact on the public conversation," he explained.

Issues like hijacked accounts have always been a part of Facebook, he added, but the overall weight of Facebook, when it comes to its impact on disinformation and political processes, is making these types of issues ever more important to the public.

"Social media has become an integral part of people's daily lives, especially when it comes to acquiring information that influences not only consumer decisions but political decisions, as well," he added.