Facebook still has a big problem with cybercrime groups

Forgers, identity thieves, spammers, and scammers have been using Facebook to hawk their services, even after a crackdown last year, according to a new report. Cisco cybersecurity research division Talos says it found dozens of Facebook groups that were “shady (at best) and illegal (at worst)”, with names like “Facebook hack (Phishing)” and “Spammer & Hacker Professional.” The groups have been shut down, but Talos is calling on Facebook to police shady groups more proactively, complaining that it’s “apparently relied on these communities to police themselves.”

Talos’ report highlights 74 groups with a total of 385,000 members. Facebook users could look up the groups by searching for keywords, including “spam” or “carding,” and Talos says that if a user joined one, Facebook would often automatically recommend related groups — “making new criminal hangouts even easier to find.” Some members advertised stolen credit card numbers by posting the victims’ driver’s licenses, and others posted requests for help transferring large sums of money or getting access to computer networks.



Some sellers appeared to simply be scamming buyers, not offering real services. But Talos linked some of the posts with real spam or phishing campaigns. Facebook has had a long-running problem with cybercrime. In 2018, security researcher Brian Krebs found 120 private groups with 300,000 members offering botnets, fraudulent tax refunds, and other illegal services. Facebook removed the groups soon after being alerted. But another researcher, Justin Shafer, alerted *Motherboard* to even more examples — some of which had been operating for years. Talos says it found several new operations with names that were "remarkably similar, if not identical" to those on Krebs' list.

Facebook tells *The Verge* that it removed the groups after Talos exposed them, and it's continuing to look for any related groups or accounts. "These groups violated our

policies against spam and financial fraud and we removed them. We know we need to be more vigilant and we're investing heavily to fight this type of activity," said a spokesperson. It says most of the groups were created in 2018.



Talos offers a less flattering account of the takedowns, saying that Facebook's abuse teams initially left some groups up, opting only to remove specific posts. "Eventually, through contact with Facebook's security team, the majority of malicious groups was quickly taken down, however new groups continue to pop up, and some are still active as of the date of publishing," it says.

Facebook has more than 2 billion users, and it's not surprising that criminals would try to attract customers there. (Groups can also be abused in more subtle ways: addiction support pages, for instance, can be exploited by

predatory treatment centers.) The big question is how these bad actors can be removed more quickly — or prevented from creating these groups in the first place. For now, Talos says it’s continuing to work with Facebook on identifying groups for removal.

Update 11:30PM ET: *Clarified that Talos is a division of Cisco.*

https://www.theverge.com/2019/4/5/18296687/facebook-cisco-talos-cybercrime-spam-scam-identity-theft-groups-takedown