Facebook urged to control the spread of US law enforcement fake accounts

Reference: Memo [190424-1] Date: 24/04/2019 - Version: 1.0
Keywords: Facebook, Social media, US
Sources: publicly available information

Key Points

- US Immigration and Customs Enforcement used fake accounts on Facebook to identify people committing immigration fraud.
- The agency created social media profiles for a non-existent university and its staff.
- All this activity violates Facebook's policies but the involved US agencies have shown no concern.
- Facebook is urged to curb the proliferation of undercover law enforcement accounts on the social media platform.

Summary

According to The Guardian, the US Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) is running a network of inauthentic social media accounts and profiles in an attempt to identify potential immigration fraudsters. These social media entities include a non-existent university called the University of Farmington. This entity has reportedly been set up by the DHS to identify people who plan to commit immigration fraud and has led to arrests of 161 people.

After the information about the University of Farmington became public, Facebook took down the related accounts. The company also commented that "Law enforcement authorities, like everyone else, are required to use their real names on Facebook and we make this policy clear on our public-facing Law Enforcement Guidelines page. Operating fake accounts is not allowed, and we will act on any violating accounts."

The digital rights group Electronic Frontier Foundation (EFF) has urged Facebook to do more in order to cut back the proliferation of undercover law enforcement accounts on the social network. According to EFF, taking down inauthentic accounts after having learned of them on the press is not good enough and a more proactive approach is needed.

Recently, Facebook has had several problems with guarding their users' privacy. According to reports, they harvested the email contacts of 1.5 million users without their knowledge or consent when they opened their accounts. Additionally, Facebook admitted to storing millions of Instagram user passwords internally without encryption. This means that Facebook employees highly likely had access to them.

Comments

Law enforcement agencies routinely use fake profiles, known as "sock puppets", in their work. It is apparent from this case that the US agencies in discussion have little regard to Facebook's user policy and are likely to continue to ignore the requirement to use their real names on social media platforms. It is also likely that some of the agencies have internal policies that prohibit their employees from using their own identities in state security related work on social media. This is a fundamental conflict in principles and is unlikely to be resolved any time soon.

As in many previous cases and despite showing willingness to tackle the problems, Facebook is again under criticism from various entities for tardiness and reactive behaviour in enforcing their own user policies. Accordingly, pressure from digital rights groups such as EFF is unlikely to relent and has led Facebook to put additional effort into tackling such situations more efficiently.

For more on Facebook and inauthentic behaviour please see CERT-EU Memos 190118-1 and 190306-1.