TEC.006

5.1.2.e

**Van:** 5.1.2.i @fb.com>
**Verzonden:** woensdag 6 mei 2020 16:57
**Aan:** 5.1.2.e ;5.1.2.e
**Onderwerp:** Facebook April Coordinated Inauthentic Behavior Report

As a partner of our security escalation channel, we would like to share our April report on enforcement actions taken against coordinated inauthentic behavior and our latest efforts on combating COVID-19 misinformation.

## Coordinated Inauthentic Behavior

We removed 8 networks that operated 732 Facebook accounts, 793 Pages, 200 Groups, and 162 Instagram accounts. These networks originated from 1) Russia, 2) Iran, 3) USA, 4) USA, 5) Mauritania, 6) Myanmar, 7) Georgia, and 8) Georgia. You can find the April report here. Previous reports can be found here.

## Combating COVID-19 Misinformation

Ever since the World Health Organization (WHO) declared COVID-19 a global public health emergency, we've been working to connect people to accurate information and taking aggressive steps to stop misinformation and harmful content from spreading. The following is a list of updates on how we are combating COVID-19 misinformation.

- Keeping People Safe and Informed About the Coronavirus
- An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19
- Addressing Deceptive Advertising Practices
- Keeping WhatsApp Personal and Private
- Combating COVID-19 Misinformation Across Our Apps

## Facebook Security Escalation Channel

As a reminder, please use this channel to report suspicious activities or issues concerning cyber/infosecurity, disinformation, or other potential platform abuses on Facebook, Instagram, Messenger and WhatsApp. Please review the guidelines below on how to report via the EMEA Security Escalation Channel.

Only email addresses that have been reviewed and approved by Facebook will be able to report to 5.1.2.i @fb.com. To ensure you receive emails from 5.1.2.i @fb.com, please whitelist or add to your approved sender list.

## Reporting Guidelines:

- This channel is solely for the reporting of cyber/info security issues, information operations, disinformation, threat actors, suspicious activities, and other potential platform abuses on Facebook, Instagram and WhatsApp.
- This is **not a legal reporting channel**. If you would like to report on potential violations of local electoral laws in the context of the elections, please use our Government Casework channel (only for electoral regulators who have been granted access) or our legal reporting channel. You may also use the legal reporting channel to report on other unlawful content posted on Facebook.
- This is **not a data request channel**. In order for Facebook to disclose data, you must first provide formal legal process via our data request portal (in accordance with law enforcement guidelines). Please note that Facebook is bound by the Stored Communications Act, 18 U.S.C. § 2701 et seq. and will release data only as legally permitted/required.
- Send reports in English. If non-English text are included, please include an English translation, if possible.

- Be as specific as possible as to what content you are reporting (e.g. if it is a Page, link to the Page) and explain why you believe it is in violation of our Community Standards or Policies. To help expedite our investigation, please provide actionable information, including:
    - Context for what you are reporting
    - Full URL links of the Page(s), Group(s), profile(s), post(s), photo(s) or video(s) you are reporting. (see here for more information on how to obtain URL links)
    - Facebook Account, Page or Group ID numbers
    - In the case of a long video, provide exact time of abuse (for example, hate speech violation at 3:45)
    - If you are reporting an account for impersonation, please provide the URL to the original profile of the person who is claiming to be impersonated or other information to help us identify the real person.
    - IP addresses
    - Web domains
    - Source of information, if coming from another party and may be shared
    - Email addresses, phone numbers or other contact details of suspected bad actors (in accordance with GDPR and any other governing legal considerations)
    - Any other indicators with a Facebook/IG/WA nexus that would benefit from additional investigation by our internal teams.
    - Indicate if this content has already been reported elsewhere. If so, where? Provide URL links and/or screenshots of where else it has been reported.
- Our team will review reports as quickly as possible, prioritizing our work according to the seriousness of the situation and will provide email updates as we progress.

**For more information on how we tackle problematic content, please read:**

- How We Respond to Inauthentic Behavior on Our Platforms: Policy Update
- Remove, Reduce, Inform: New Steps to Manage Problematic Content

**Other Useful Resources:**

- Newsroom: https://newsroom.fb.com/
- Hard Questions: https://newsroom.fb.com/news/category/hard-questions/
- Hacked Accounts: https://www.facebook.com/help/131719720300233/ or http://www.facebook.com/hacked
- Impersonation: https://www.facebook.com/help/www/174210519303259
- Facebook Safety Centre: https://www.facebook.com/safety
- Facebook Security Tips: https://www.facebook.com/about/security
- Tips to Spot False News: https://www.facebook.com/help/188118808357379
- Community Standards: https://www.facebook.com/communitystandards/
- Terms and Policies: https://www.facebook.com/policies/
- Ads about Social Issues, Elections and Politics: https://www.facebook.com/business/help/167836590566506?id=288762101909005