Anti-Scam Bounty

Task 5: Takedowns of other forms of scams (browser extensions, apps, social media accounts) (recurring)

The goal of this task is to augment Task 1 with finding and taking down other forms of scam such as browser extensions, apps and social media accounts that pose a threat to users' of DOT or KSM.

Eligible members

- Current implementers of the Anti-Scam Bounty, Community moderators and Polkadot Ambassadors.

- Legal entities (companies) that specialize in this field

- Individuals can work as teams for this bounty. In that case, they need to declare it to the curator and specify a new account to receive the bounty. The account needs to have an on-chain identity. The distribution of the bounty among the members of the team is up to them.

- Legal entities can acquire a "power of attorney" from Web3 Foundation and/or Parity to file DMCAs for trademarks held by W3F and/or Parity. In the future, if other projects/foundations join the initiative they can provide similar "power of attorney" statements for their respective trademarks.

Current implementers

Currently, two members of the community, all moderators on Discord that are already part of the current community initiative have expressed interest in participating as implementers:

- Frankywild (13YWynHAu8F8uKZFbQwvPgJ67xizvo21HCEQU3Ke8z1XHoyT)
- Tim Janssen (1pHpxvp2CYscDreozYQdBkJkUkLFQftxQTAwMs5M1a6GRBf)

The implementers will work as a team, both reporting the submissions and taking actions to flag and take them down.

The invitation to participate has not been extended to companies at this point. However, the curator reached out to some social media companies (Telegram, Facebook, Twitter) through email to find out how to take down scams on their platforms but didn't get any response for that. We will work with ways of reporting scams as found in their FAQs.

Curator

The member of the community that will assume the duties of curator is Maimunat Ibrahim, Polkadot Ambassador and Community Moderator for Polkadot and Kusama Discord servers (Mims4life#4745 on Discord).

Account: 15DPQskycLALmFjGnsB212D1oxDJC2NscHeC65kaWnK62Pcm
Verified on-chain identity: BERRYZ

Rewards

- **Implementers reward**: $80 per take down
  The rewards are based on takedowns and flagging. For telegram, flagging a group, channel and bot as **scam** is enough to get the reward.

  Whoever finds (submits) the scam gets 60% of the reward and the other implementers who take down the scams share the remaining 40% equally.

  For duplicate submissions, only the first one counts. The rewards will be awarded to their individual wallet addresses, not a multisig, based on the reward formula above.

- **Curator reward:** $10 per submission + $800 per month for the first 3 months and $500 after that, for the management of the bounty. The reward for the first 3 months has been set higher to account for the efforts to kick start the task.

N/B: Sometimes, these takedowns take a long time to happen, the participants can also take mitigating actions (takedown of the backend endpoints, post comments warning users etc). These actions *can* be rewarded with *additional* rewards as stated above, if indeed the takedown turns out to take a long time.

Payout

This is a recurring task. On the first of each month (or close to it)the curator of the bounty will report the aggregated numbers of browser extensions, apps and social media accounts submitted and taken down by each implementer, along with the rewards they should receive and their own fee.

After reviewing the submission, the General Curator will open one child bounty for each implementer soon after. As soon as it’s accepted by the Child Curator, the bounty can be paid out.

Submission Process

1) The implementer fills out the Google form that automatically fills out the spreadsheet.Immediately after submission, the implementer starts employing all necessary actions to take down scam links of browser extensions, apps and social media accounts.
2) The curator then checks each link for liveness and, if it's live, compares its content to the proof provided. Any live sites that are not live are marked as such by the curator in the column provided for that in the spreadsheet.
3) The curator checks again for liveness at mid-month and at the end of the month for any links that have not been verified as taken down.
4) On the first of each month, the curator must fill out the **"Monthly rewards"** sheet.

N/B: In situations where two or more implementers submit the same link(s) and screenshot(s), implementers will be rewarded based on who submitted first by checking the screenshot of the site with the date and time of the system clock visible, as proof of the liveness of the site at the time of submission.

Eligible Browser extensions /Apps/ Social Media Accounts

Any browser extensions, social media accounts and apps that pose a threat to DOT or KSM users are considered valid for submission. More specifically these include;

1. Fake social media account support profiles for Twitter, Telegram, Discord, Facebook and Youtube as well as those that post comments under posts made by official Polkadot, Kusama , Web3 Foundations and Parity Technologies accounts across the various social media platforms listed above.
2. Any copycat of the official Polkadot, Kusama, Web3 Foundation or Parity Technologies social media accounts on platforms such as Telegram, Twitter,

Facebook, Discord and YouTube which have evidence of scams. In such situations, both the links found in their public chat groups and accounts should be reported and taken down.

3. Phishing extensions that pose a threat to users of DOT or KSM should be reported and taken down.If the scam is not clear, it is the implementers' duty to prove a specific extension is phishing.
4. Instances of Parity Signer installers (or imitations of it) on third-party apk providers. Parity Signer should be allowed to be distributed only through the official Google and Apple app stores. Also, for mobile apps, only Parity Signer is eligible at this moment. Other wallets are not eligible but may be included as we expand this task down the line.

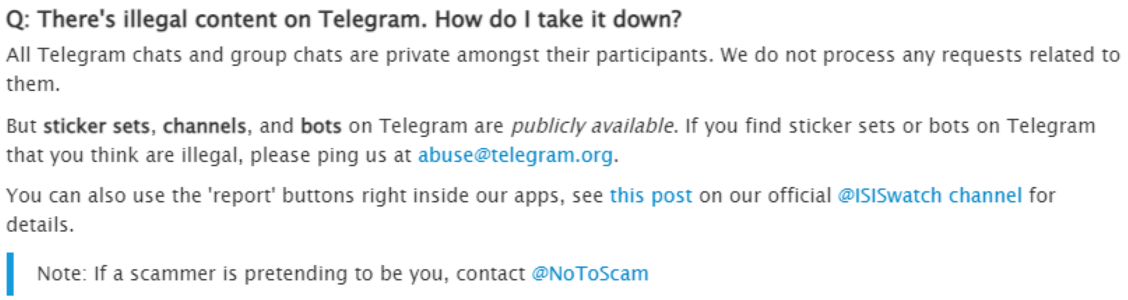
Ineligible Browser extensions /Apps /Social Media Accounts

At this point, the bounty only covers browser extensions, apps and social media accounts targeting Polkadot and Kusama. The following are considered invalid;

1. Social media accounts created by community members especially those used by Ambassadors to represent and promote Polkadot and Kusama activities in their respective regions (Example Polkadot India, Polkadot Africa, Polkadot Espanol, Polka Haus, DotsamaHub,etc). However, any community social media profile should contain content relative to our ecosystem. Profiles that use the name or logo but post unrelated content, or try to pass as official, **are eligible.**
2. Those impersonating parachains or posing a threat to holders of their tokens (both native and non-native tokens).
3. Those posing a threat to DOT or KSM *pegged* tokens on other chains.
4. Those impersonating other projects in the ecosystems (with exception that they pose threat to DOT or KSM users).
5. Investment scam browser extensions, apps and social media accounts that just list assets such as DOT and KSM without asking for users' mnemonic phrases or otherwise attempting to compromise the users' accounts.

Screenshots and FAQs links on how to report scam for the various social media platforms.

A) **Telegram - https://telegram.org/faq**



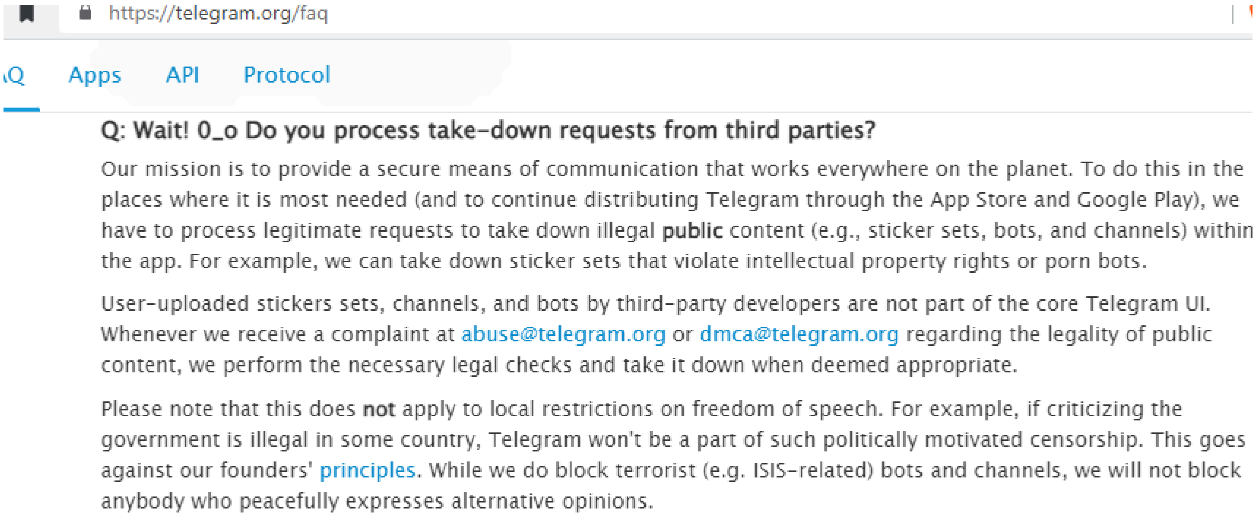
Q: There's illegal content on Telegram. How do I take it down?

All Telegram chats and group chats are private amongst their participants. We do not process any requests related to them.

But **sticker sets**, **channels**, and **bots** on Telegram are *publicly available*. If you find sticker sets or bots on Telegram that you think are illegal, please ping us at abuse@telegram.org.

You can also use the 'report' buttons right inside our apps, see this post on our official @ISISwatch channel for details.

> Note: If a scammer is pretending to be you, contact @NoToScam



Q: Wait! 0_o Do you process take-down requests from third parties?

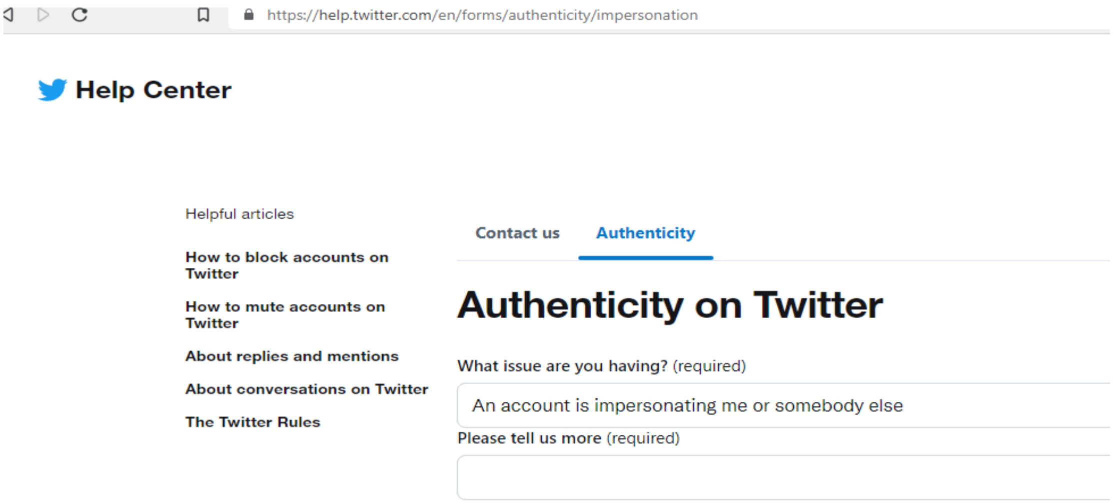
Our mission is to provide a secure means of communication that works everywhere on the planet. To do this in the places where it is most needed (and to continue distributing Telegram through the App Store and Google Play), we have to process legitimate requests to take down illegal **public** content (e.g., sticker sets, bots, and channels) within the app. For example, we can take down sticker sets that violate intellectual property rights or porn bots.

User-uploaded stickers sets, channels, and bots by third-party developers are not part of the core Telegram UI. Whenever we receive a complaint at abuse@telegram.org or dmca@telegram.org regarding the legality of public content, we perform the necessary legal checks and take it down when deemed appropriate.

Please note that this does **not** apply to local restrictions on freedom of speech. For example, if criticizing the government is illegal in some country, Telegram won't be a part of such politically motivated censorship. This goes against our founders' principles. While we do block terrorist (e.g. ISIS-related) bots and channels, we will not block anybody who peacefully expresses alternative opinions.

B) **Twitter- https://help.twitter.com/en/forms/authenticity/impersonation**

https://help.twitter.com/en/safety-and-security/phishing-spam-and-malware-links



https://help.twitter.com/en/forms/authenticity/impersonation

Help Center

Helpful articles

How to block accounts on Twitter

How to mute accounts on Twitter

About replies and mentions

About conversations on Twitter

The Twitter Rules

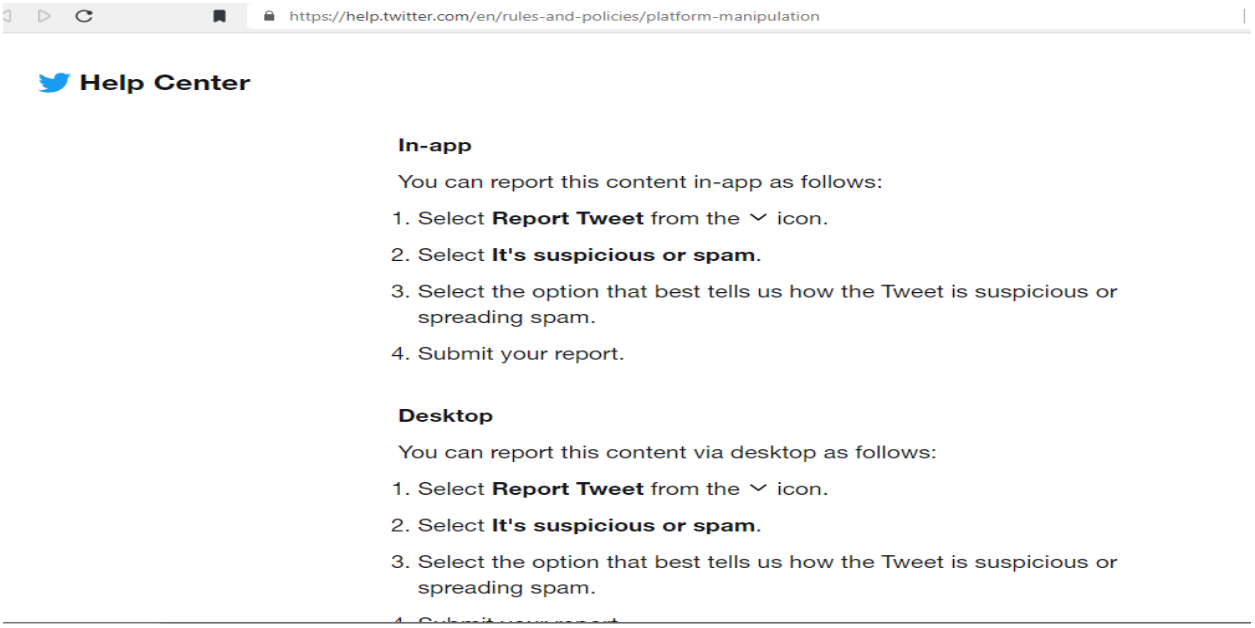
Contact us | Authenticity

Authenticity on Twitter

What issue are you having? (required)

An account is impersonating me or somebody else

Please tell us more (required)



https://help.twitter.com/en/rules-and-policies/platform-manipulation

Help Center

In-app

You can report this content in-app as follows:

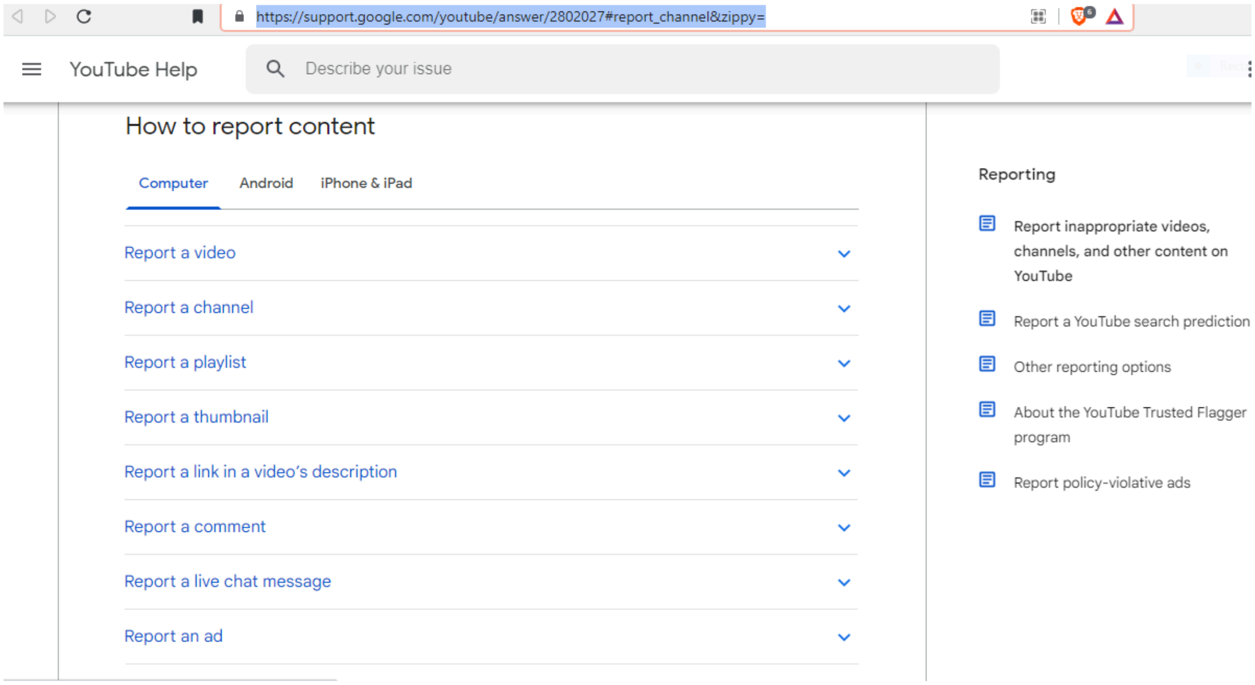
1. Select **Report Tweet** from the ⌄ icon.
2. Select **It's suspicious or spam**.
3. Select the option that best tells us how the Tweet is suspicious or spreading spam.
4. Submit your report.

Desktop

You can report this content via desktop as follows:

1. Select **Report Tweet** from the ⌄ icon.
2. Select **It's suspicious or spam**.
3. Select the option that best tells us how the Tweet is suspicious or spreading spam.
4. Submit your report

C) YouTube- https://support.google.com/youtube/answer/2802027#report_channel&zippy=



https://support.google.com/youtube/answer/2802027#report_channel&zippy=

YouTube Help

Describe your issue

How to report content

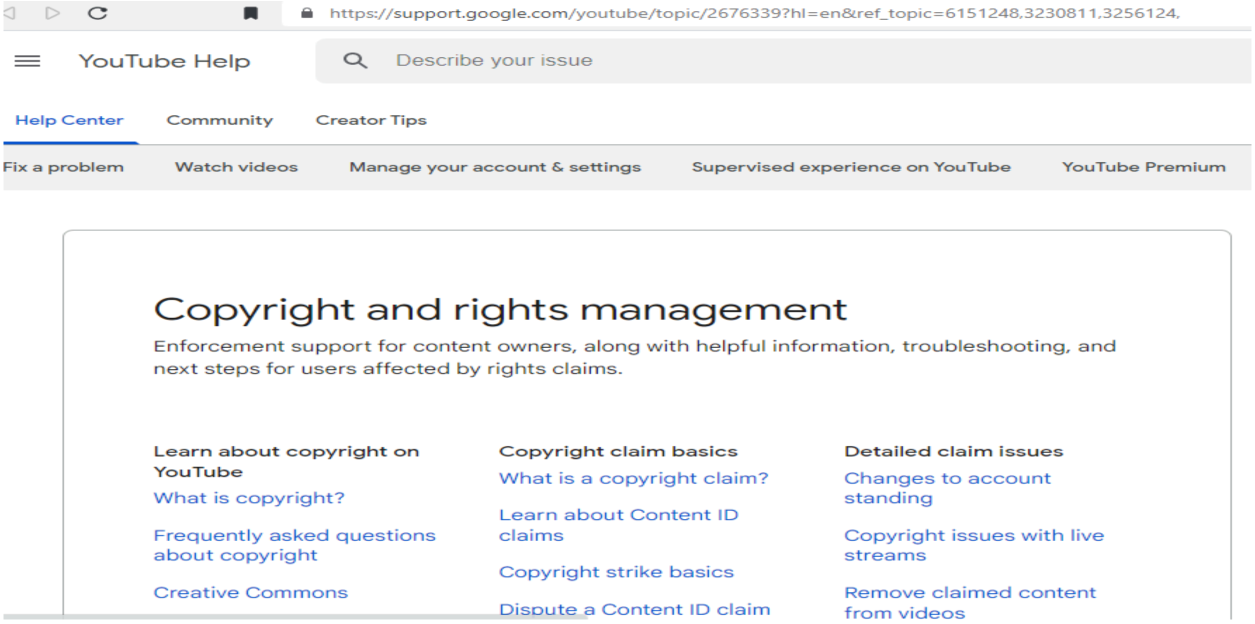
Computer | Android | iPhone & iPad

- Report a video
- Report a channel
- Report a playlist
- Report a thumbnail
- Report a link in a video's description
- Report a comment
- Report a live chat message
- Report an ad

Reporting

- Report inappropriate videos, channels, and other content on YouTube
- Report a YouTube search prediction
- Other reporting options
- About the YouTube Trusted Flagger program
- Report policy-violative ads

https://support.google.com/youtube/topic/2676339?hl=en&ref_topic=6151248,3230811,3256124,



https://support.google.com/youtube/topic/2676339?hl=en&ref_topic=6151248,3230811,3256124,

YouTube Help

Describe your issue

Help Center | Community | Creator Tips

Fix a problem | Watch videos | Manage your account & settings | Supervised experience on YouTube | YouTube Premium

Copyright and rights management

Enforcement support for content owners, along with helpful information, troubleshooting, and next steps for users affected by rights claims.

Learn about copyright on YouTube

What is copyright?

Frequently asked questions about copyright

Creative Commons

Copyright claim basics

What is a copyright claim?

Learn about Content ID claims

Copyright strike basics

Dispute a Content ID claim

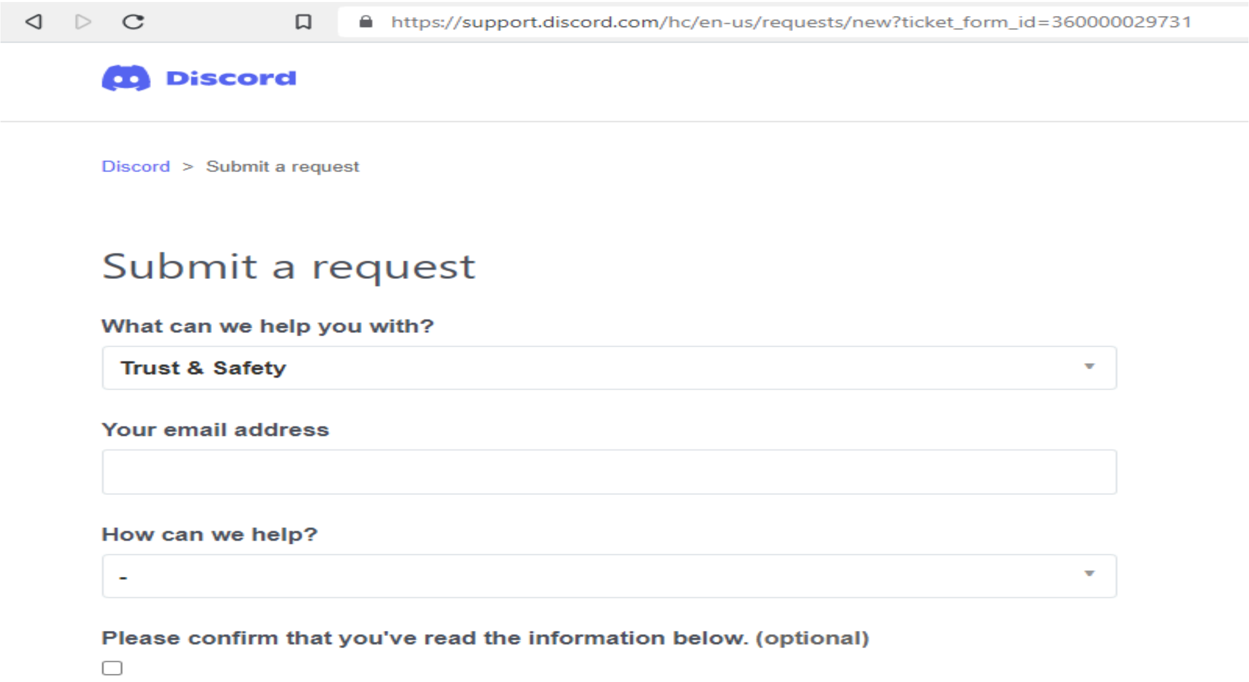
Detailed claim issues

Changes to account standing

Copyright issues with live streams

Remove claimed content from videos

D) Discord - https://dis.gd/request



https://support.discord.com/hc/en-us/requests/new?ticket_form_id=360000029731

Discord

Discord > Submit a request

Submit a request

What can we help you with?

Trust & Safety

Your email address

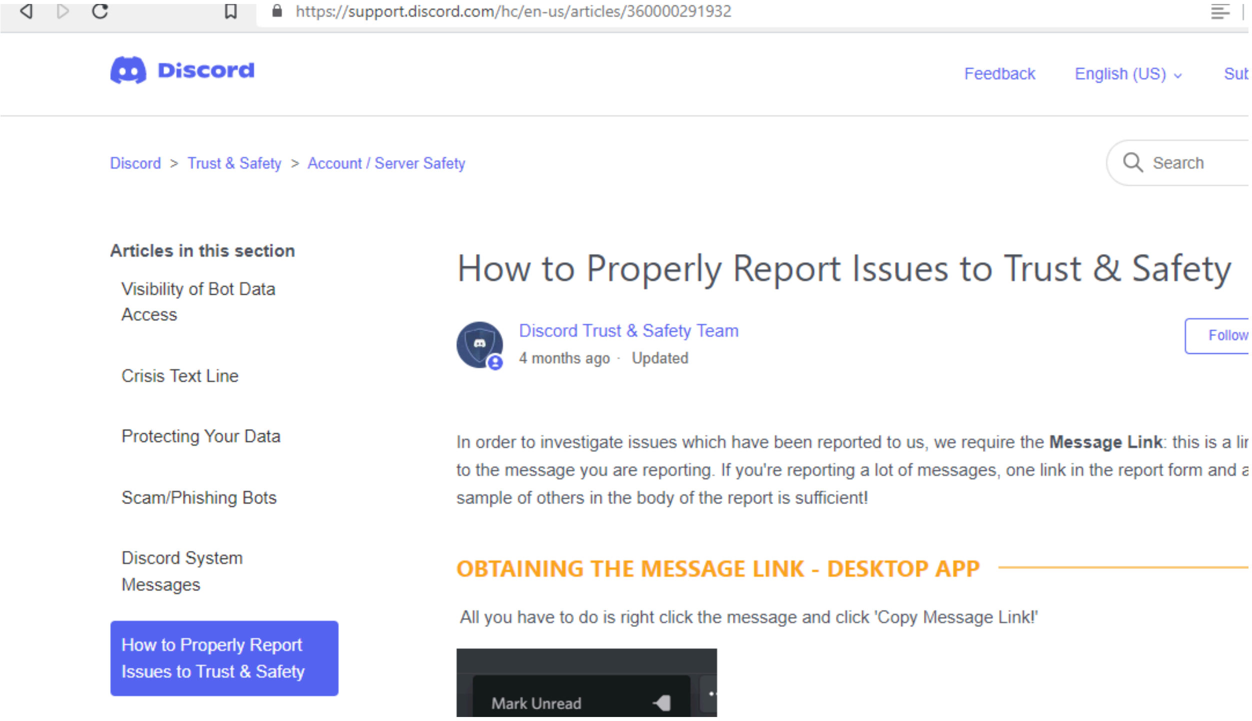
How can we help?

-

Please confirm that you've read the information below. (optional)

□

https://dis.gd/howtoreport



https://support.discord.com/hc/en-us/articles/360000291932

Discord

Discord > Trust & Safety > Account / Server Safety

Articles in this section

- Visibility of Bot Data Access
- Crisis Text Line
- Protecting Your Data
- Scam/Phishing Bots
- Discord System Messages
- How to Properly Report Issues to Trust & Safety

How to Properly Report Issues to Trust & Safety

Discord Trust & Safety Team

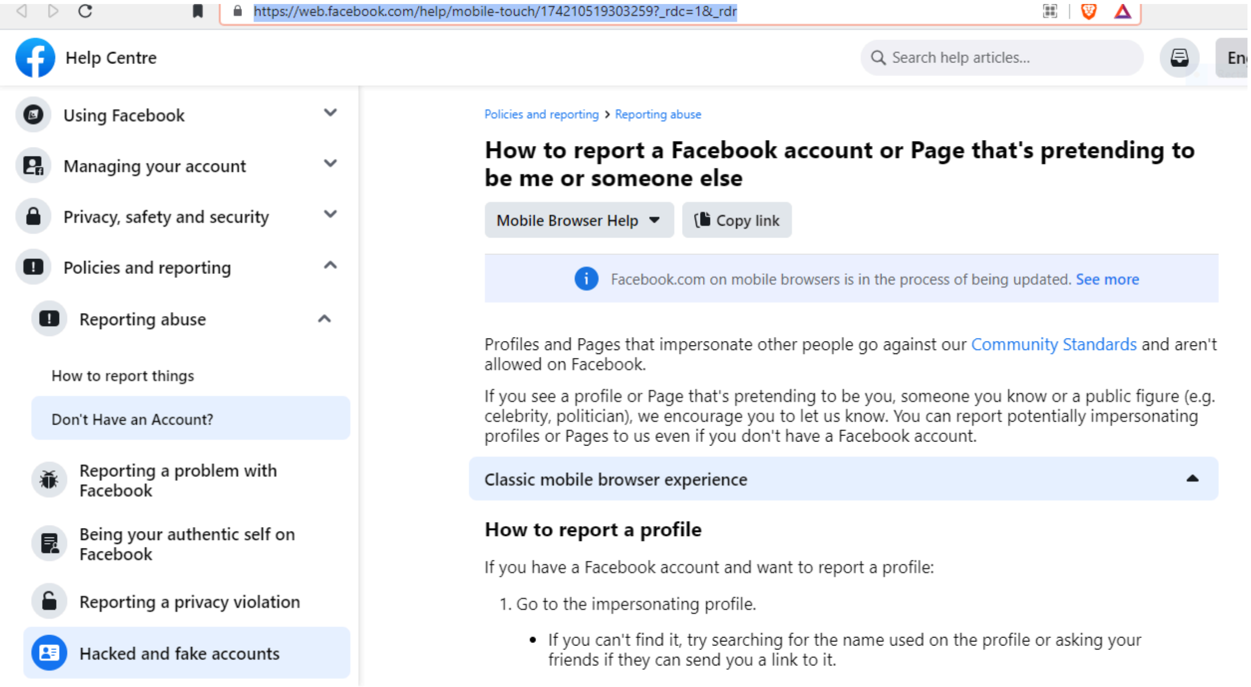
4 months ago · Updated

In order to investigate issues which have been reported to us, we require the **Message Link**: this is a lir to the message you are reporting. If you're reporting a lot of messages, one link in the report form and a sample of others in the body of the report is sufficient!

OBTAINING THE MESSAGE LINK - DESKTOP APP

All you have to do is right click the message and click 'Copy Message Link!'

E) Facebook- https://web.facebook.com/help/174210519303259/?helpref=uf_share



Policies and reporting > Reporting abuse

How to report a Facebook account or Page that's pretending to be me or someone else

Facebook.com on mobile browsers is in the process of being updated. See more

Profiles and Pages that impersonate other people go against our Community Standards and aren't allowed on Facebook.

If you see a profile or Page that's pretending to be you, someone you know or a public figure (e.g. celebrity, politician), we encourage you to let us know. You can report potentially impersonating profiles or Pages to us even if you don't have a Facebook account.

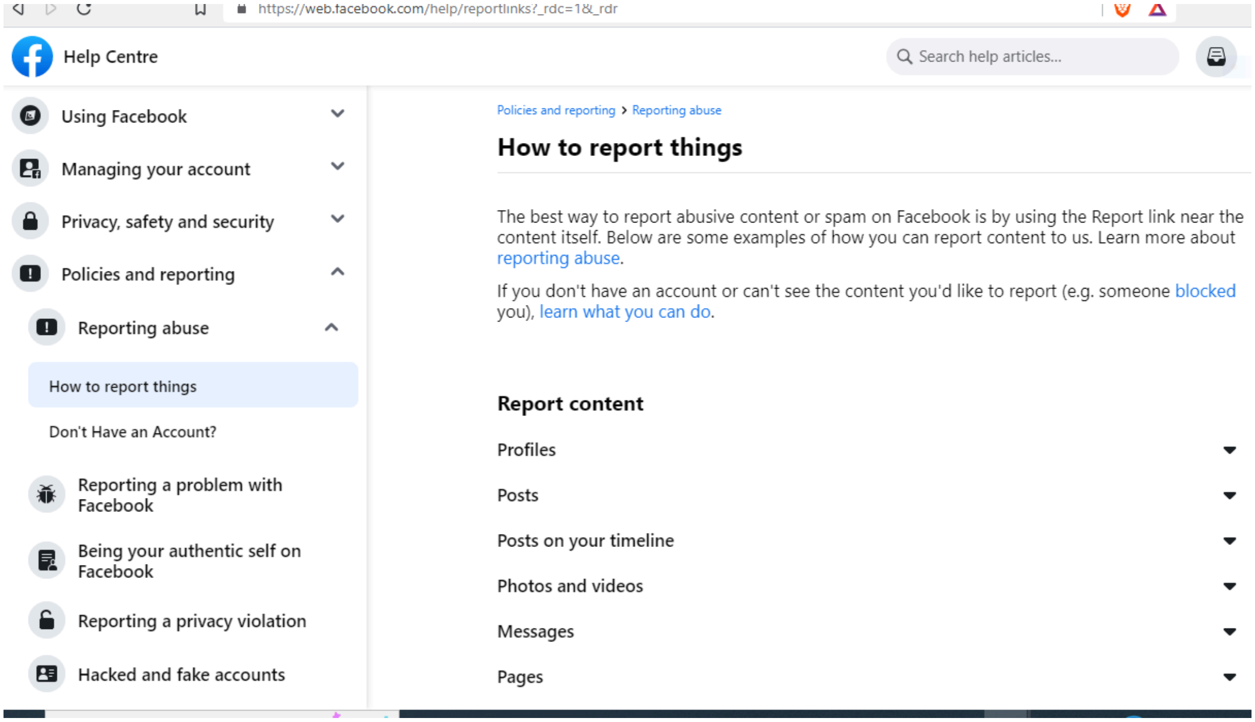
Classic mobile browser experience

How to report a profile

If you have a Facebook account and want to report a profile:

1. Go to the impersonating profile.
   - If you can't find it, try searching for the name used on the profile or asking your friends if they can send you a link to it.

https://www.facebook.com/help/reportlinks



https://web.facebook.com/help/reportlinks?_rdc=1&_rdr

Help Centre

Search help articles...

- Using Facebook
- Managing your account
- Privacy, safety and security
- Policies and reporting
  - Reporting abuse
    - How to report things
    - Don't Have an Account?
  - Reporting a problem with Facebook
  - Being your authentic self on Facebook
  - Reporting a privacy violation
  - Hacked and fake accounts

Policies and reporting > Reporting abuse

How to report things

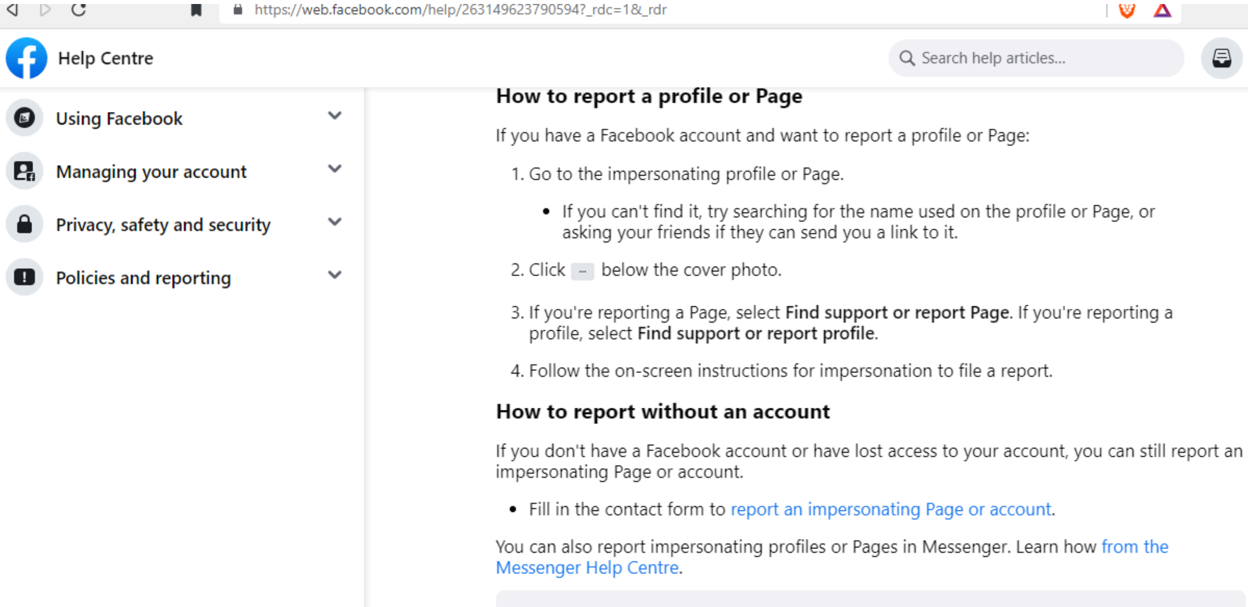
The best way to report abusive content or spam on Facebook is by using the Report link near the content itself. Below are some examples of how you can report content to us. Learn more about reporting abuse.

If you don't have an account or can't see the content you'd like to report (e.g. someone blocked you), learn what you can do.

Report content

- Profiles
- Posts
- Posts on your timeline
- Photos and videos
- Messages
- Pages

https://web.facebook.com/help/263149623790594?_rdc=1&_rdr



https://web.facebook.com/help/263149623790594?_rdc=1&_rdr

Help Centre

Search help articles...

- Using Facebook
- Managing your account
- Privacy, safety and security
- Policies and reporting

How to report a profile or Page

If you have a Facebook account and want to report a profile or Page:

1. Go to the impersonating profile or Page.
   - If you can't find it, try searching for the name used on the profile or Page, or asking your friends if they can send you a link to it.
2. Click ··· below the cover photo.
3. If you're reporting a Page, select **Find support or report Page**. If you're reporting a profile, select **Find support or report profile**.
4. Follow the on-screen instructions for impersonation to file a report.

How to report without an account

If you don't have a Facebook account or have lost access to your account, you can still report an impersonating Page or account.

- Fill in the contact form to report an impersonating Page or account.

You can also report impersonating profiles or Pages in Messenger. Learn how from the Messenger Help Centre.