

Distribution of hacked materials policy



1. [Help Center](https://help.twitter.com/) ^
2. [Platform integrity and authenticity](https://help.twitter.com/en/rules-and-policies#platform-integrity-and-authenticity) ^

Distribution of hacked materials policy

Overview

October 2020

The use of hacks and hacking to exfiltrate information from private computer systems can be used to manipulate the public conversation, and makes all of us less secure online. We do not condone attempts to compromise or infiltrate computer systems. As such, we don't permit the use of our services to directly distribute content obtained through hacking by the people or groups associated with a hack. In addition, we may label Tweets containing or linking to hacked materials to help people understand the authenticity or source of these materials and provide additional context.

Note: Other portions of the [Twitter Rules](https://help.twitter.com/rules-and-policies/twitter-rules) (https://help.twitter.com/rules-and-policies/twitter-rules) may apply to material obtained through hacking, or to the actions of individuals associated with a hack. For example:

- Our private information policy (<https://help.twitter.com/rules-and-policies/personal-information>) covers the sharing of private information without consent, regardless of how the private information was obtained.
- Our private information policy (<https://help.twitter.com/rules-and-policies/personal-information>) also covers threats, bounties, or encouragement to expose someone's private information, including through hacking.
- Our non-consensual nudity policy (<https://help.twitter.com/rules-and-policies/intimate-media>) covers the sharing of intimate photos or videos of someone that were produced or distributed without consent.

What is in violation of this policy?

We define a hack as an intrusion or access of a computer, network, or electronic device that was unauthorized or exceeded authorized access. Behaviors associated with the production of materials which would count as a hack under this policy include:

- Unauthorized access or interception, or access that exceeds authorization (for example, from an insider), to a computer, network or electronic device, including breaches or intrusions
- Disclosing materials accessed legitimately outside of approved systems or networks
- Disclosing materials where there is evidence that they were obtained through malware or social engineering

We use a range of evidence to establish that a hack has taken place, including reports from the victims of the hack, claims of responsibility by a hacker or hacking group, information provided by third parties (including law enforcement), our own systems and data where available and relevant, and other credible publicly-available information.

We define hacked materials as the information obtained through a hack. Information need not be personally-identifiable private information in order to qualify as hacked materials under this policy.

The distribution of materials includes:

- posting hacked content on Twitter (e.g., in the text of a Tweet, or in an image); and
- posting Tweets which include links to hacked content hosted on other websites.

Direct distribution of real or synthesized hacked materials

Under this policy, we do not allow the people or groups directly associated with a hack to use Twitter to distribute hacked materials.

The people or groups directly associated with a hack include:

- the hackers or hacking groups themselves
- the representatives (official or self-identified) of or proxies acting in direct coordination with the hackers or hacking groups
- the employers or funders of the hackers

Indirect distribution of real or synthesized hacked materials

Under this policy, we may label or apply warning messages to Tweets containing or linking to real or synthesized hacked materials where these Tweets do not constitute direct distribution (as defined above).

What is not a violation of this policy?

We recognize that source materials obtained through leaks can serve as the basis for important reporting by news agencies meant to hold our institutions and leaders to account. As such, we defer to their editorial judgement in publishing these materials, and believe our responsibility is to provide additional context that is useful in providing clarity to the conversation that happens on Twitter.

In most cases, discussions of or reporting about hacking or hacked materials constitutes indirect distribution (unless the people or groups directly associated with a hack are responsible for the production of the discussions or reporting). In these cases, a violation of this policy would result in a label or warning message,

not removal of the Tweet(s) from Twitter.

Additionally, this policy only addresses instances in which the materials themselves are being distributed — not discussions of or reporting about hacking which refer to but do not embed or link to the materials themselves. Tweets referring to a hack or discussing hacked materials would not be considered a violation of this policy unless materials associated with the hack are directly distributed in the text of a Tweet, in an image shared on Twitter, or in links to hacked content hosted on other websites.


Who can report violations of this policy?

Anyone can report the distribution of materials obtained through hacking, whether they have a Twitter account or not. In some cases, we may need to hear directly from the owner of the information being shared (or an authorized representative, such as a lawyer) before taking enforcement action.

How can I report violations of this policy?


In-app

You can report this content for review in-app as follows:

1. Select **Report Tweet** from the  icon.
2. Select **It's abusive or harmful**.
3. Select **Includes private information**.
4. Select the type of information that you're reporting.
5. Select the relevant option depending on who owns the information you are reporting.
6. Select up to 5 Tweets to report for review.
7. Submit your report.

Desktop

You can report this content for review via desktop as follows:

1. Select **Report Tweet** from the  icon.
2. Select **It's abusive or harmful**.
3. Select **Includes private information**.
4. Select the type of information that you're reporting.
5. Select the relevant option depending on who owns the information you are reporting.
6. Select up to 5 Tweets to report for review.
7. Submit your report.

You can also report this content for review via our [private information report form](https://help.twitter.com/forms/private_information) (https://help.twitter.com/forms/private_information) by selecting the type of private information that you want to report.

What happens if you violate this policy?

Accounts engaged in the direct distribution of hacked materials which are found to be directly operated by hackers, hacking groups, or people acting for or on behalf of such hackers will be permanently suspended.

In cases where accounts engaged in the direct distribution of hacked materials are operated by proxies for hackers or hacking groups, but are not directly controlled by such hackers, we may require the deletion of specific Tweets that directly distribute hacked materials, or permanently suspend accounts for repeated violations.

If you believe that your account was locked or suspended in error, you can [submit an appeal](https://help.twitter.com/forms/general?subtopic=suspended) (<https://help.twitter.com/forms/general?subtopic=suspended>).

We will also block links to websites operated by the hackers, hacking groups, or people acting for or on behalf of such hackers which directly distribute hacked materials.

We may provide additional context on Tweets which indirectly distribute hacked materials (as defined above) where they appear on Twitter. This means we may:

- Apply a label and/or warning message to the content where it appears in the Twitter product;
- Show a warning to people before they share or like the content;
- Provide a link to additional explanations or clarifications, such as in a Twitter Moment or relevant Twitter policies.

Where we have evidence that a hack, or the distribution of hacked materials, was conducted or facilitated by a state-backed actor, or that the materials in question may be manipulated, we may also reduce the visibility of the content on Twitter and/or prevent it from being recommended.

Typically, we will take these actions on all Tweets engaging in indirect distribution of hacked materials, regardless of the author of the Tweet.

Additional resources

Learn more about our [range of enforcement options](https://help.twitter.com/rules-and-policies/enforcement-options) and our approach to [policy development and enforcement](https://help.twitter.com/rules-and-policies/enforcement-philosophy).

Learn more about [private information](https://help.twitter.com/rules-and-policies/personal-information) and our [election integrity efforts](https://about.twitter.com/en_us/values/elections-integrity.html).

Share this article



Was this article helpful?^{*}



Submit