

Detected malicious attack campaign targeting TikTok, threatening to delete accounts of many celebrities

International security researchers have recently issued an urgent warning about a new phishing attack campaign on the TikTok platform.

In particular, the threat actors mainly target the famous [TikTok](#) account, which has a lot of followers, interactions, and belongs to the people with great influence on this social networking site.

As revealed by researchers from Abnormal Security team, who first discovered the malicious campaign, there were 2 peak attack periods recorded in this campaign: On October 2nd. and November 1, 2021. Observing campaign email distribution shows that attack cycles tend to peak every 3-4 weeks. Hence a new 'loop' will most likely start in just a few weeks.

In some of the cases noted by Abnormal Security, malicious actors often impersonated TikTok employees to send emails to targets, threatening that their accounts were about to be deleted due to alleged violations of the general terms of the app. communication.

From Omer Faruk <omerf200021@gmail.com> ☆
Subject [LIKELY PHISHING] TikTok Team #536328439 1:01 PM
To emily.paranaguana@gmail.com emily.paranaguana@gmail.com mullham@stymptre 44 more
To protect your privacy, Thunderbird has blocked remote content in this message. Preferences X

Support | Copyright

This e-mail was sent by TikTok officials. Please reply

Hi dear user,

Your account violates our Copyright. Complainant Firm: Yunitec LTD. © All Rights Reserved. Your account will be deleted

from copyright within 48 hours, will not be re-entered If you think this is an error and you do not want your account

deleted Please reply to this email with "Confirm My Account".

Copyright is very important to us. If necessary actions are not taken from our connection,

you will be removed from our servers within 48 hours. Please do not change your password while your account is being examined

Support Account ID: #60696731942

© TikTok Inc., [1601 Willow Road, Menlo Park, CA 94025 USA \[google.com\]](#)

Another element of deception commonly used by hackers in spoofing emails is providing a 'Verified' badge for added credibility and authenticity. TikTok's 'Verified' badge is crucial to content posted by verified accounts, and is a signal that the platform's algorithm will increase the impression share of posts coming from these accounts. Using this scam is simple yet very effective, as many people will be delighted to receive an email offering them a chance to receive a verification badge from the platform. But that is not the case at all.

From honda Berlin <hondaberlingalery@gmail.com> ☆
Subject [LIKELY PHISHING] TikTok Team #74948 10/2/21, 4:14 AM
To [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] 85 more

--External Sender--

TikTok Verified Badge

This e-mail was sent by TikTok officials. Please reply.

Hi dear user,



The account caught our attention and we examined the account. We saw that he shared his own original content. We offer the right to receive a verified badge for your account.

To get a verified badge for your account, you must verify that you are the real owner of the account. We will give you a form to verify that you are the true owner of the account.

To receive the verification form for your account, reply to this email by typing 'Verify My Account'.

In either case, the attackers would provide the target with a method to verify their account: Clicking a link embedded in the spoofed email. Of course this is also a malicious link. Upon clicking this link, victims are redirected to a [WhatsApp](#) chat room, where they are greeted by a scammer posing as a TikTok employee.

After a few messages back and forth, the scammer will eventually ask the victim for an email address, phone number, and otp code that passes multi-factor [authentication](#) and resets the account's password.



Account hijacking or extortion?

At the moment, it is not clear what the real motives of the scammers in this campaign are. But more likely this could be an attempt to take over valuable accounts, or to blackmail the account owner.

TikTok's terms of service state that if an account, especially one with a lot of followers, violates the platform's general rules, it will be suspended or permanently locked. This means that after taking over a victim's account, malicious actors can easily threaten to post something inappropriate, resulting in the account being locked.

Regardless of the attackers' motives, if you own or manage valuable social media accounts, make sure to back up all your content and data in one safe place. Additionally, you should always secure your account with [two-factor authentication](#) (2FA) or 2-step verification. Ideally, use a hardware security key. At the same time, you should also be wary of unusual emails sent to your account.

You finished reading the article "**Detected malicious attack campaign targeting TikTok, threatening to delete accounts of many celebrities**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.