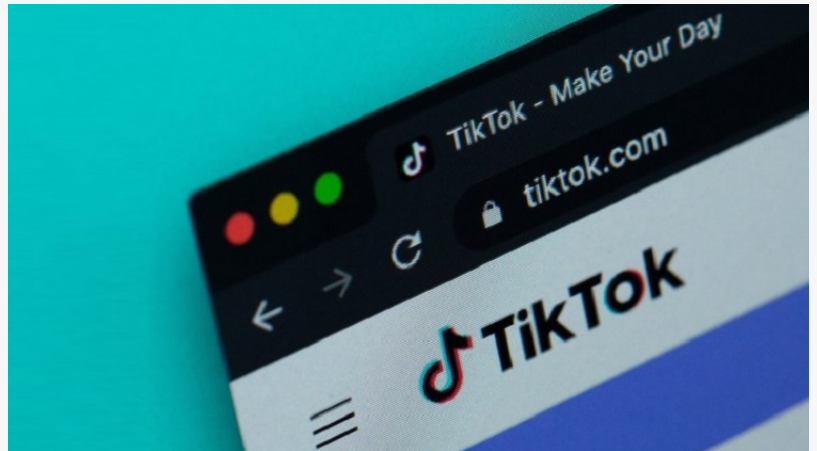


TikShock: Don't get caught out by these 5 TikTok scams

DUBAI, DUBAI, UNITED ARAB
EMIRATES, September 12, 2022

/EINPresswire.com/ -- Are you aware of the perils of the world's no. 1 social media, asks Jake Moore, the Global Security Advisor for [ESET](#) and he further probes do you know how to avoid scams and stay safe on TikTok?

TikTok continues to shock us all by breaking records and widening its audience, yet unfortunately with such a broad reach, scammers inevitably remain not too far behind. In only six years it has become the dominant social media platform for sharing and viewing short videos and now boasts that viewers in the UK and US are spending more time on TikTok than on YouTube.



Cybercriminals are very creative and always follow trends closely, even predicting change before the masses in order to maximize the outcome of their techniques. Not too many years ago, there were only a few platforms to use to target new victims while leaving little evidence and unlikely to face any repercussions. The dark web became a place to buy and sell contraband, but the numbers didn't ever really hit the relative big time with the audiences such that those taking advantage of the technology could actually achieve their wildest dreams.

Con artists have seen the growth in social media coming and soon began using various platforms to carry out scams of all sorts. TikTok has over 1.2 billion daily users, so the numbers are there for the taking. Furthermore, while in an app that people are scrolling minute after minute, even hour after hour, scams can easily catch people off guard and often make them lose money, their account, or even their reputation.

TikTok scams to look out for

Get-rich-quick and crypto scams

Con artists love to lure people in with claims of huge rewards in return for little effort.

Cryptocurrencies have boomed (and plummeted) in recent times so they tend to generate a lot of noise online and TikTok remains a favorite when attempting to part people from their cash. These offers always sound too good to be true – that is because they are. Is Elon Musk really going to give random web strangers a million dollars?

TikTok phishing messages

A TikTok scam email or text is a message that goes out at random like a typical phishing message, but in the hope that they land in a TikToker's inbox. They might try to offer a verified badge, more followers, or even a sponsorship. Once the target clicks on the link in the message, the victim will be redirected to a site requesting TikTok login credentials. If it does not have two-factor authentication (2FA) enabled (which TikTok accounts do not, by default), once these details have been handed over, the hackers will have control of the account and could even lock the genuine user out.

Bot accounts

TikTok is, unfortunately, still full of bot accounts that cleverly interact with users in a way that make the targeted users think they are chatting with a real person. These bots may ultimately ask victims for sensitive information or even suggest the victims be redirected to a site that is in fact a scam site attempting to phish information from them or install malware on their phones.

TikTok scam apps

Fake accounts on TikTok sometimes promote apps that are available to download. The problem is that these apps are also in fact fake. Some accounts will claim that specific paid-for apps can be downloaded free from certain third-party app stores. However, in an attempt to steal your information, these apps will actually install malware or adware on your device.

Fake celebrities

Some accounts may attempt to impersonate real celebrities. This is usually completed by simply duplicating the content of a celebrity's account. This is an attempt to get as many followers as possible, and before they are found out and reported they may use the platform to promote further scams such as cryptocurrency investment scams.

Staying safe on TikTok

While hacking into someone's TikTok remains tricky without being near the target's phone and carrying out a spot of shoulder surfing, it is a good reminder to make sure you have 2FA turned on. This helps keep cybercriminals at bay should they ever be able to see the reset code sent to your mobile because it will also require the code sent to your email address as well.

Like other platforms, TikTok will never contact you asking for your account details, password, one time passcode, or any other verification methods. Due to the scale of the problem, it is vital that you remember to keep an eye out for scammers who are probably going to try to trick you into sharing your personal information, usually by email or through an in-app message.

Finally, if you ever see videos on TikTok that you think could be spam or possibly attempting to phish people for information, report them to TikTok straight away and steer clear of any associated links.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/590438152>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 Newsmatics Inc. All Right Reserved.