Staying safe on TikTok: How to avoid being scammed or hacked

Issued by ESET

3 Nov 2022

It's the world's number one social media platform, which also means it's the biggest target for scammers, hackers and shady characters. Carey van Vlaanderen, CEO of ESET South Africa shares a few tips and insights on what to avoid to stay safe.


Carey van Vlaanderen, CEO of ESET SA

Launched in 2016, TikTok has 6.44 million active users currently in South Africa above the age of 18, which is no small feat in comparison to Facebook which has been running since 2006 with 24.20 million users in the country. With such a broad reach, scammers are never far behind. Cybercriminals are exceptionally creative with their tactics and always follow trends closely, often predicting change ahead of the masses in order to increase the likelihood of their scams being successful. However, scams are not the only dangers lurking on the popular video-sharing application, and users would do well to know how to stay safe while enjoying themselves. Given that it's so easy to lose track of time scrolling the app, it's not hard for scams to catch people off guard, which can cause them to lose money, their account, or even their reputation.

Top TikTok scams to be aware of and avoid

1. **Don't be fooled by get-rich-quick and crypto scams**
   Is Elon Musk really going to give random web strangers a million dollars? Is a worldwide brand really going to give away a luxury vehicle just for following a new account? Unlikely. If it sounds too good to be true, it usually is. Con artists are known for luring people into their web of deceit with offers of huge reward for little effort. Cryptocurrencies have skyrocketed (and hit rock bottom) recently, so they remain a favourite topic for scammers when attempting to part unsuspecting people from their cash. Competitions and giveaways must be carefully scrutinised. Even if they're not looking to scam you out of money, your personal information could be just as useful to a scammer looking to commit identity theft.

2. **Don't click those TikTok phishing messages**
   A TikTok scam email or text is a message that goes out at random, like a typical phishing message, but with the intention of landing in a TikToker's inbox. Such a message might purport to offer a verified badge, more followers, or even a brand sponsorship. Once the target clicks the link in the message, they will be redirected to a site requesting TikTok login credentials. If the user does not have two-factor authentication (2FA) enabled (which TikTok accounts do not, by default), the hackers can take complete control over the account and lock the owner out completely, using their login details.

3. **Don't engage with bot accounts**
   Despite their best efforts, TikTok is still unfortunately rife with 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.

4. **Don't get caught by TikTok scam apps**
   Fake accounts on TikTok often 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 onto your device. Avoid downloading any additional apps that do not come from an official app store.

5. **Don’t fall for fake celebrities**
   Some accounts attempt to impersonate real celebrities. They usually do this by duplicating the content of a celebrity’s account. This tactic is used to get as many followers as possible. Before the scammer is caught out and reported, they may use this account to promote further scams such as cryptocurrency investment scams. Alternatively, scammers use this account to gather as many followers as quickly as possible, and then switch to a personal account, so that they can exploit their now-high follower account by monetising or promoting other scams.

Staying safe on TikTok

While hacking into someone’s TikTok is challenging without being near the target’s phone and carrying out a spot of shoulder surfing, it is a good reminder to make sure that 2FA is turned on. This makes it harder for cybercriminals as they might be able to see the reset code sent to your mobile number (using spyware) but it’s unlikely they’ll have access to your second authenticating medium (email) as well.

Other important safety tips

- Never share your login details with anyone:
  Like other platforms, TikTok will never contact you asking for your account details, password, one time passcode, or any other verification methods.
- Make your account private:
  This means that the content you post on the account is not visible to anyone you do not know.
- Only allow friends to send messages:
  Don't accept messages from strangers. If you only accept messages from friends, you don’t have to worry about the intent behind their message.
- Don't suggest your account to others:
  Turning off 'Suggest your account to others' will keep your account from attracting random users you don't know. It will also stop your TikTok account from coming up in search engine results.
- Don't allow people to download your videos:
  There's a feature that lets other users download the videos you share on your channel. Turning this off helps ensure that no one uses your content, image, or identity in a way you wouldn't want it to be used.
- Limit comments:
  Cyberbullying is a huge safety issue these days, and it can happen to anyone. By disabling comments, you can ensure that no one uses your platform to say unkind or hurtful things to you or anyone else.

Finally, if you ever see videos on TikTok that you think could be spam or phishing attempts, or you see any harmful content, report it to TikTok straight away and avoid the associated links or accounts.

- **Eset launches solution to address SOHO security concerns** 15 Apr 2024
- **Don’t gamble with your cybersecurity** 29 Feb 2024
- **Avoiding job scams, and finding a job you love** 9 Feb 2024
- **Sharenting and security concerns: Will you be posting that back-to-school photo?** 10 Jan 2024
- **Fighting the digital grinch: Cybersecurity tips for kids and parents for a safe festive season** 8 Dec 2023

ESET

ESET has been helping people protect their digital worlds for more than three decades. From a small, dynamic company we've grown into a global brand with over 110 million users in 202 countries.
Profile | News | Contact | Twitter | Facebook | RSS Feed