

# [***Is Telegram a National Security Threat? | Opinion***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:6BPG-9961-JBR6-92HS-00000-00&context=1516831)

Newsweek.com

April 2, 2024 Tuesday 10:41 AM EST

Copyright © 2024 Newsweek Inc. All Rights Reserved



**Length:** 814 words

**Byline:** John Mac Ghlionn

**Highlight:** There is very little, if anything, secure about Telegram, contrary to popular reports.

**Body**

The U.S. is fixated on [*TikTok*](https://www.newsweek.com/topic/tiktok?utm_source=Synacor&utm_medium=Attnet&utm_campaign=Partnerships). The Chinese app, we're told, is a national security threat. It is a danger to the American people. Some suggest that it is part of a sinister scheme orchestrated by the Chinese government to manipulate U.S. ***politics*** and exacerbate the existing deep divisions within the country. In fact, I [*suggested this*](https://www.nationalreview.com/2021/06/tiktok-is-chinas-trojan-horse/) many years ago. However, by obsessing over one app, we run the risk of forgetting about the dangers posed by other apps, like Telegram. In the U.S. alone, it has close to [*11 million*](https://backlinko.com/telegram-users) monthly active users, [*many of whom*](https://membit.io/blog/who-uses-telegram-whatsapp-imessage-and-other-instant-messengers/) are young, impressionable individuals.

The Russian-made app, according to a new report from [*Guardio*](https://labs.guard.io/scammers-paradise-exploring-telegrams-dark-markets-breeding-ground-for-modern-phishing-a2225e51898e), has, in recent times, evolved into a thriving center where experienced cybercriminals and beginners can openly share illegal tools and knowledge—a "scammers paradise." As a result, a dark and well-organized supply chain of tools and victims' data has emerged. Within this ecosystem, one can find not only free samples, tutorials, and kits on Telegram, but even hackers-for-hire, offering everything needed to construct a complete, end-to-end malicious campaign.

In other words, as the report noted, the phishing system has been democratized.

For the uninitiated, the term "phishing" is used to describe an effort to fraudulently obtain sensitive information, such as usernames, passwords, credit card numbers, bank account details, or other valuable data, with the intention of using or selling the acquired information.

This is something that should concern every single Telegram user in the U.S. Phishing destroys lives. A [*recent digital privacy survey report*](https://www.usnews.com/360-reviews/privacy/digital-privacy-consumer-survey) found that 61 percent of American survey respondents had their personal data compromised at some point in their lives. Additionally, 44 percent have experienced this multiple times. The [*most common form*](https://www.stationx.net/phishing-statistics/#:~:text=1.,trillion%20phishing%20emails%20per%20year.) of cyber crime, phishing is on the rise. Last year, 36 percent of data breaches in the United States were attributed to phishing attacks. In 2023, [*71 percent*](https://www.proofpoint.com/us/blog/security-awareness-training/2024-state-of-phish-report#:~:text=In%202023%2C%2071%25%20of%20organizations,of%20damage%20to%20their%20reputation.) of all companies in the U.S. were victims of a successful phishing attack. The health care sector, rich in sensitive data, is[*particularly vulnerable*](https://expertinsights.com/insights/healthcare-cyber-attack-statistics/) to phishing attacks.

Which brings us back to Telegram, a messaging app that, according to its website, prides itself on providing users with high levels of privacy and security.

As the Guardio report clearly demonstrated, there is very little, if anything, secure about Telegram, contrary [*to popular reports*](https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html).

The report comes at a time when Pavel Durov, the CEO of Telegram, is, according to reports, considering a potential initial public offering (IPO) in the U.S. In a recent interview with the [*Financial Times*](https://www.ft.com/content/8d6ceb0d-4cdb-4165-bdfa-4b95b3e07b2a), Durov indicated that going public could be a viable option in the coming years.

Since its inception, a little over a decade ago, Durov has gone to great lengths to position his platform as a privacy-focused alternative to Big Tech behemoths. He has argued that Telegram could become a sanctuary for individuals residing in oppressive regimes and that he and his colleagues would "protect user data at any cost."

More than [*a billion people*](https://www.bankmycell.com/blog/number-of-telegram-users/)in the U.S. and beyond, worried about the dominance of major tech players and their privacy, bought what he was selling. In many ways, these people, including myself, were sold a lie.

The paradox lies in Telegram's emphasis on its security and privacy features, despite there being[*no automatic end-to-end encryption in place*](https://www.kaspersky.com/blog/telegram-why-nobody-uses-secret-chats/46889/); instead, message protection relies on policies rather than technology. Such a security flaw poses a risk to your privacy, and the availability of malware for hire poses a threat to your device. This becomes even more glaring when considering that[*Google Messages*](https://www.zdnet.com/article/google-messages-just-got-a-major-security-upgrade/#:~:text=End%2Dto%2Dend%20encryption%20is,what%20that%20means%20for%20you.&text=Android%20and%20iPhone%20users%20have,versus%20RCS%20feud%20for%20years.) and [*Facebook Messenger*](https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/#:~:text=End%2Dto%2Dend%20encryption%20helps%20protect%20your%20privacy%20by%20ensuring,they%20reach%20the%20receiver's%20device.) now offer default end-to-end encryption.

As Jeff Allen, co-founder and chief research officer for the Integrity Institute, a U.S think-tank, recently [*told the*](https://www.ft.com/content/c70ef7d6-230a-4404-b854-2e75fe0f2e0a) [*Financial Times*](https://www.ft.com/content/c70ef7d6-230a-4404-b854-2e75fe0f2e0a), in addition to "broader integrity issues," people "should be worried about the criminal underworld" that exists on Telegram.

He's right. They should.

That's because Telegram is, in many ways, [*the new "dark web."*](https://www.bitdefender.com/blog/hotforsecurity/telegram-becomes-the-new-dark-web-for-cybercrime/) However, unlike the traditional dark web, which requires specialized browsers, Telegram is considerably easier to access. In truth, there are no barriers to entry. Simply download the app, and away you go. Enter a world of unimaginable filth and crime.

Users can use Telegram, now a mix of [*Reddit*](https://www.newsweek.com/topic/reddit?utm_source=Synacor&utm_medium=Attnet&utm_campaign=Partnerships), Rumble, 4Chan, and Craigslist to buy just about anything, from [*abortion pills*](https://www.wired.com/story/telegram-abortion-pill-market/), [*Bolivian cocaine, and fraudulently cloned bank cards.*](https://www.ft.com/content/c70ef7d6-230a-4404-b854-2e75fe0f2e0a)

Telegram may be safe for organized criminals, but it's not safe for everyday Americans. TikTok is not the only dangerous app in existence. U.S. lawmakers would do well to remember this rather important fact.

*John Mac Ghlionn writes about social issues, technology, and the impact of media manipulation. Follow him* [*@ghlionn*](https://twitter.com/ghlionn)*.*

*The views expressed in this article are the writer's own.*

[*Link to Image*](https://d.newsweek.com/en/full/2371669/logo-telegram.jpg)

**Graphic**

Logo of Telegram

Chesnot/Getty Images

The logo of the social media application Telegram is displayed.

**Load-Date:** April 2, 2024

**End of Document**