valencia

September 13, 2024

Profile Suspended

The Telegram CEO’s Arrest, Content Moderation, and You

How the Russian Zuckerberg Got Filtered Out

In late August, we learned that Telegram's CEO was arrested when landing in France. Pavel Durov was detained at Paris-Le Bourget Airport and released after four days on bail of 5 million euros. He is required to report to a police station twice a week. In response to his arrest, Telegram has stated that it follows EU laws and its content moderation practices are improving.

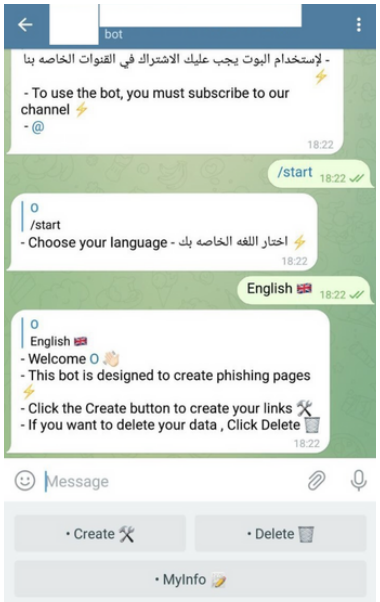
Since its foundation, Telegram has kept growing in popularity across the globe. With his reputation as the founder of Vkontakte, Russia's answer to Facebook, Durov soon made Telegram the main messaging app across the Russian-speaking world. Notably, both Russian and Ukrainian armed forces use Telegram to communicate.

Since the early 2020s, Telegram has also become known as a haven for cybercrime. Telegram's content moderation is seen by many as lax, meaning that the platform quickly became a trading platform to barter for a variety of criminal offerings, including illegal pornography, drug sales, and stolen goods. In this context, Telegram also opens unwitting users to many cybersecurity risks.

Telegram and the Case of the Missing Encryption

Telegram is unlike other messaging apps such as WhatsApp or Signal. It's true in the sense that the organization rarely cooperates with law enforcement. This was exemplified in 2023, with WhatsApp submitting over 1.3 million CyberTipline reports while Telegram submitted none. It's also true in that, unlike Signal or WhatsApp, Telegram chats are not end-to-end-encrypted by default and users must go activate the function in their app settings. Further, Telegram group chat communications cannot be encrypted. They also allow as many as 200,000 people, which makes it one of the greatest vectors for the spread of misinformation considering that the app still platforms a long list of political extremists.

First and foremost, though, Telegram remains a platform for cybercriminals. Hackers openly sell stolen credentials through the application and use its bots to help create phishing pages:



bot

- لإستخدام البوت يجب عليك الاشتراك في القنوات الخاصه بنا
⚡

- To use the bot, you must subscribe to our channel ⚡
- @

18:22

/start 18:22 ✓✓

O
/start
- Choose your language - اختار اللغه الخاصه بك ⚡

18:22

English 🇬🇧 18:22 ✓✓

O
English 🇬🇧
- Welcome O 👋
- This bot is designed to create phishing pages ⚡
- Click the Create button to create your links 🛠
- If you want to delete your data , Click Delete 🗑

18:22

Telegram is also often used to create phishing landing pages, imitating login pages for widely used services such as Microsoft, UPS, and many more. In 2023, researchers from NetSkope showed how Telegram is even used by hackers to steal credentials and bypass multi-factor authentication.

Telegram Tactics: Sending Cyber Risks Packing

Much of the discussion around Telegram echoes chatter about the banning of TikTok. Should you use Telegram? We recommend that you'd switch to a safer, end-to-end-encrypted messaging service. Here are some steps for individuals and organizations to consider about Telegram:

1. Lock it down. If you must use Telegram, turn on end-to-end encryption in the app's settings. Don't join groups that look suspicious and be aware that everything you say in your groups is not encrypted. Be wary of unexpected invitations, unprompted contacts, and bots. Telegram's "Secret Chat" function has end-to-end-encryption enabled by default; use it.
2. Frame it up. Decide and enshrine what your and your organizations' approach to Telegram is. Does it constitute reasonable personal use? Is it properly framed by your IT security policy framework? Do users know not to share files via Telegram? Is it clearly and thoroughly addressed in your Acceptable Use Policy?
3. Do Not Trust. Remember, this is an unencrypted platform with a history of abuse. By highly suspicious of new interactions on Telegram.

While Telegram remains a popular messaging platform, its lax content moderation and lack of default end-to-end encryption exposes users to significant cyber risks. For both individuals and organizations, it’s crucial to implement strict security measures, such as enabling encryption features, exercising caution in group interactions, and establishing clear policies to mitigate these risks.