Common thieves usually throw out the SIM card immediately (the phone is harder to locate this way), then wipe the devices and sell them, so there isn't much risk for the data in case of regular petty theft. But if you have reasons to worry about the data on the device and are unable to log out the other device, it is best that you wipe it remotely. You can read more about it here: Apple iOS, Android. Unfortunately, this requires you to have prepared in advance for this scenario.

You can delete your Telegram account if you are logged in on at least one of your other devices (mobile or desktop). Note that inactive Telegram accounts self-destruct automatically after a period of time — 6 months being the default setting.

Bots

> If you're a developer, you may find our Bots FAQ more useful.

Q: What are bots?

Bots are like small programs that run right inside Telegram. They are made by third-party developers using the Telegram Bot API.

Q: How do I create a bot?

Creating Telegram bots is super-easy, but you will need at least some skills in computer programming. If you're sure you're up to it, our **Introduction for Developers** is a good place to start.

Unfortunately, there are no out-of-the-box ways to create a working bot if you are not a developer. But we're sure you'll soon find plenty of bots created by other people to play with.

Q: A bot is sending me messages, how do I make it stop?

If you don't want a bot to send you messages, feel free to block it – same as you would block a human user. Some Telegram clients have a 'Stop Bot' button right in the bot's profile.

That said, most bot developers offer commands that silence the bot, check its */help* for clues.

Q: Are bots safe?

Yes. Bots are no different from human users that you meet in groups for example. They can see your public name, username, and profile pictures, and they can see messages you send to them, that's it. They can't access your last seen status and **don't** see your phone number (unless you decide to give it to them yourself).

Naturally, any bot should be treated as a stranger — don't give them your passwords, Telegram codes or bank account numbers, even if they ask nicely. Also, be careful when opening files sent by bots, same as you would deal with ordinary humans. Example: If a bot sent us a file called *OpenMe.exe*, we probably wouldn't open it.

Q: If I add a bot to my group, can it read my messages?

Bots can work in two modes when you add them to groups. By default, bots only see messages that are meant for them. In this case, you'll see 'has no access to messages' in the group members list next to the bot.

Some bots need more information to work, so developers may disable the privacy mode. In this case, the bot will see all messages sent to the group, and you will see 'has access to messages' in the members list next to the bot.

Learn more about privacy mode for bots »

If your group contains very sensitive information, maybe it's better to avoid adding bots you don't trust 100%.

Q: Are bots made by Telegram?

No. While we have some official bots for specific purposes (like @gif or @Stickers, we don't usually make bots. Bots are made by third-party developers using the Telegram Bot API and platform.

Q: Where can I find more bots?

There is no official store at the moment, so you'll have to ask your friends or search the web for now. We're pretty sure you'll find some bots to play with.

Deeper questions

Q: Can I get Telegram's server-side code?

All Telegram client apps are fully open source. We offer verifiable builds both for iOS and Android – this technology allows to independently verify that the application you download from the app stores was built using the **exact same code** that we publish.

By contrast, publishing the server code doesn't provide security guarantees neither for Secret Chats nor for Cloud Chats. This is because – unlike with the client-side code – there's no way to verify that the **same code** is run on the servers.