🔐 Telegram Security Checklist v2

How to protect your account — and your money — from hijacking

Most Telegram account breaches don't happen because of technical flaws.

They happen because someone was pressured into sending a code.

This checklist protects you from both technical compromise and social engineering attacks.

Updated: February 2026

🔥 STEP 1. Set up a strong Telegram password (Two-Step Verification / 2FA)

Why this matters:

An SMS code alone is not protection. If someone gains access to your phone number, they can log in.

A password adds a second lock.

What to do:

- [ ] Settings → Privacy & Security → Two-Step Verification
- [ ] Enable a password

What makes a secure password:

- [ ] At least 12 characters
- [ ] Not your name, birthday, or simple combinations
- [ ] A long phrase works best

Example:

CoffeeWithNoSugarOnTheBalcony!

> 💡 Use a password manager if needed (built-in on iPhone and Android).

🔥 STEP 2. Add a recovery email (CRITICAL)

Without a recovery email, losing your password may mean losing your account permanently.

What to do:

➡ Add a recovery email in the 2FA section

➡ Make sure:

- ☐ You can access it
- ☐ It has its own strong password
- ☐ 2FA is enabled on the email account

> 💡 Your email is your backup key.

🔥 STEP 3. NEVER share verification codes — with anyone. Ever.

This is the most important rule.

Telegram, banks, crypto wallets, and legitimate support teams

will NEVER ask you to send them your login code.

If someone asks you to:

➡ Send a 6-digit code

➡ Forward an SMS

➡ Confirm identity by replying with a code

➡ “Verify your account” urgently

It is 100% a scam.

Even if:

➡ The account looks official

➡ It has a blue badge

➡ It says “Support”

➡ It mentions account deletion

➡ It shows a “transaction warning”

> 💡 If you send the code, you are giving them access yourself.

🔥 STEP 4. Review and reset connected devices

Attackers may already be logged in silently.

What to do:

➡ Settings → Devices

➡ Check:

- [ ] Unknown countries
- [ ] Unknown devices

➡ If unsure:

- [ ] Terminate ALL sessions
- [ ] Log back in only on your own devices

🔥 STEP 5. Enable a Passkey

A passkey is a secure login method that replaces SMS codes.

It uses:

➡ Face ID

➡ Fingerprint

➡ Device PIN

Stored securely:

➡ iPhone → iCloud

➡ Android → Google

Enable it in:

- [ ] Settings → Privacy & Security → Passkey

> 💡 Even if someone knows your phone number, they cannot log in without your device.

🔐 STEP 6. Protect your phone number

SIM-swap attacks are real.

Recommended:

- [ ] Set a SIM PIN with your carrier
- [ ] Do not publish your phone number publicly

➡ In Telegram:

- [ ] Settings → Privacy → “Who can see my phone number?” → Nobody

---

⚠️ STEP 7. Adjust privacy settings

Review:

- [ ] Who can add you to groups
- [ ] Who can message you
- [ ] Who can see your last seen

> 💡 Limit access to reduce exposure.

⚠️ STEP 8. Disable automatic media download and autoplay

Why this matters:

Malicious files are often disguised as videos or documents.

What to do:

➡ Settings → Data and Storage

➡ Disable:

- [ ] Automatic media download
- [ ] Video autoplay

> 💡 It’s safer to tap “Download” manually than to fix a compromised device later.

⚠️ STEP 9. Never open links without context

Even if they come from someone you know.

Common red flags:

- ➡ “Check this urgently”
- ➡ “Is this you in the photo?”
- ➡ “Please vote here”

> 📌 Friends’ accounts are often hacked first.

⚠️ STEP 10. Be careful with fake “Support” accounts

Attackers often impersonate support services.

Red flags:

- ➡ Strange or invisible symbols in the name
- ➡ Emoji in official-looking accounts
- ➡ “Premium” badge (this is NOT verification)
- ➡ Urgent threats
- ➡ Links to unfamiliar domains

Telegram does NOT:

- ➡ Message users first
- ➡ Ask for login codes
- ➡ Ask you to send SMS codes back

⚠️ STEP 11. Always check website addresses

Look-alike domains are common.

Examples:

- ➡ te1egram.org or tg-login.net

Official domains:

- ➡ telegram.org
- ➡ t.me

> 💡 If it looks slightly wrong — do not open it.

⚠️ STEP 12. Use “Login with Telegram” carefully

Recommendations:

- ➡ Use it only on trusted and well-known websites
- ➡ Periodically review access:
  - ☐ Settings → Devices / Connected Services
  - ☐ Remove anything unnecessary

💡 Analogy:

> This is like websites you’ve given a spare key to — regularly check who still needs it.

⚠️ STEP 13. Files, PDFs and QR codes

Telegram does NOT authorize login via PDF.

PDFs or images may contain:

- ➡ Phishing links
- ➡ Fake login QR codes

> 💡 If a file asks you to log in — treat it as suspicious.

💰 STEP 14. If you use Telegram Wallet

Your Telegram account may directly control your funds.

That means:

- ➡ Account compromise = financial loss
- ➡ Crypto transactions are often irreversible

Never:

- ➡ Approve transactions under pressure
- ➡ React to “24-hour deadline” threats
- ➡ Confirm transfers because “support” asked

> 💡 Most wallet thefts happen due to social engineering — not hacking.

🛡️ STEP 15. Backups

➡ iPhone → iCloud

➡ Android → Google

Remember:

➡ Secret chats cannot be restored

➡ Important information should be saved separately

🚨 IMPORTANT REMINDERS

Telegram never:

➡ Messages users first

➡ Asks for passwords

➡ Asks for login codes

> 💡 Urgency is a manipulation tactic.

🆘 If you suspect compromise

- [ ] Terminate all sessions
- [ ] Change your password
- [ ] Check recovery email
- [ ] Enable passkey
- [ ] Warn your contacts
- [ ] If using Wallet — review recent transactions immediately

---

✋ Contact for questions

I created this checklist due to a rise in Telegram account hijackings involving social engineering and wallet theft.

If you want to review your settings or secure accounts for yourself or your team, you can message me on Telegram: **@iiaio**

I work with digital security and will try to point you in the right direction.