GetSales.io

Checklist ✅

21 LinkedIn Ban Triggers to Avoid in 2025. According to the Experts

Protect your outreach accounts and avoid LinkedIn penalties in 2025

By **GetSales, MirrorProfiles & Gologin**

Why These Triggers Actually Matter

Whether you're running 1 LinkedIn account or 100, the ban triggers we've covered aren't just theoretical edge cases — they reflect how LinkedIn's detection systems actually work. Many of these patterns are already monitored by LinkedIn's internal and external anti-spam teams, and enforcement is only getting stricter in 2025.

You can't afford to ignore them. If you lose a LinkedIn account, **recovery can take up to 2 months — and the chances of success are around 20%**.

> "**LinkedIn rarely bans you for one mistake. It bans you for patterns.** It's not that you sent X message and got banned. LinkedIn works like a penalty point system. Every suspicious action adds risk — and eventually, you cross a line".
> — Peter, co-founder of GetSales

You won't get banned for one wrong message. But combine that with bad proxy setup, session leaks, repetitive actions, low reply rates — and you're toast.

✅ Run this checklist with your team to spot hidden risks before LinkedIn does.

🚩 *= risky trigger to avoid* ✅ *= recommended safeguard*

The 5 Categories of Risk

Across LinkedIn experts all triggers fell into 5 main buckets:

1. Browser & Device Fingerprinting
2. IP, Proxy, and Session Hygiene
3. Behavioral Patterns & Timing
4. Message & Content Risks
5. Profile Quality & Perception

Browser Fingerprinting & Anti-Detect Setup

🚩 Using Chrome profiles or incognito mode

🚩 Reusing the same fingerprint across accounts

🚩 No emulation of real browsing behavior

🚩 No session persistence starting fresh logins every time

🚩 Using LinkedIn-related extensions that perform automation directly — most are blacklisted (e.g. Apollo, Lemlist)

✅ Use an anti-detect browser like GoLogin

✅ Use the right proxy setup (stable & reliable vendor & proxy type)

✅ Simulate unique device footprints — as if you're running separate laptops

> **"VPNs and proxies are not enough.** LinkedIn doesn't just see your IP — it sees your device, your installed fonts, your system language, your OS version. That's why so many people get banned even with 'clean' proxies".
> — Anton, Marketing manager at GoLogin

💡 GetSales uses Bright Data proxies by default — trusted, stable, and optimized for LinkedIn outreach.

Proxy, IP & Session Hygiene

LinkedIn tracks where, how, and when you're logging in. It flags mismatched geolocation, new sessions from different IPs, shared or blacklisted proxies, and even attempts to encrypt the traffic (hello VPNs 👋).

🚩 Multiple IPs on one account

🚩 Dirty/shared proxies

🚩 Frequent proxy or geo changes

🚩 Using VPNs with encrypted traffic

✅ Use 4G mobile or static high-quality proxies

✅ Avoid risky IPs

✅ Work from tools with native session protection (like GetSales + GoLogin)

Behavioral Patterns & Activity Design

LinkedIn's anti-spam filters are smarter than ever. It looks at how you behave: timing, pace, rhythm.

🔹 Launching with **new accounts**? Warm-up takes time.

> “If you're **launching outreach with fresh accounts**, be ready: LinkedIn takes time to trust them. It usually takes 2–3 months”.
> — Peter, co-founder of GetSales

🔹 Before any outreach: behave like a human.

Even **aged accounts** need time to adapt to new patterns. You can’t just start sending outreach at full speed. That’s why GetSales has a built-in warm-up & ramp-up engine:

- We score each profile to assess risk level.
- We automatically assign daily limits and gradually increase them.
- You can set a Server Schedule to control when profiles are active — mimicking real.

> **“Even your 'Like' speed matters** — if you like too fast, you don’t look like a beginner, you look like a bot”.
> – Frédéric, co-founder of MirrorProfiles

🚩 No warm-up period

🚩 Sudden spike in activity

🚩 Same number of messages daily

🚩 Same number of connection requests daily

🚩 24/7 online status

🚩 No variation in actions
(e.g. 0 engagement, just connects)

🚩 Never withdrawing old invites

✅ Always warm up even aged accounts (2 weeks before launching the first campaign)

✅ Randomize all actions: number, timing, sequence

✅ Use tools like GetSales that throttle activity based on health score

✅ Monitor reply and block rates

✅ Withdraw stale connection requests regularly

Messaging & Content Triggers

It’s not just what you send — it’s when and to whom. Sending links to cold leads? Spam. Long blocks of text? Spam. Same message every time? You get the idea.

🚩 Links in the first message or if they haven’t replied

🚩 Low reply rate across the board

✅ Avoid links until after the lead replies

✅ Watch your reply:request ratio

✅ Only use tools with smart enrichment like GetSales, that are not using your accounts directly to enrich leads from your campaigns

✅ Keep messaging human, relevant, and brief

✅ Use spintax to generate unique versions of your messages — GetSales supports this natively

Profile Quality & Realism

> **“LinkedIn doesn’t just ban bots. It bans unbelievable humans.** If your account looks fake, your connection request will get reported — and that alone can trigger a ban”.
> — Frédéric (MirrorProfiles)

🚩 Suspicious photos (AI-generated, mismatched ethnicity/location)

🚩 Unrealistic job history or credentials

🚩 Zero content or mutual connections

🚩 Recycled bios and work history across accounts

✅ Use real-looking AI photos that pass detection tests

✅ Match profile region, language, and niche

✅ Focus on credibility, not perfection (especially <500 connections)

✅ Avoid obvious fake names or job descriptions

⚠️ Early Ban Signals

These early indicators are your chance to pause, reassess, and fix what’s going wrong before you get hit with a full restriction. Don’t ignore them. If any of these appear, stop your outreach activity, review your account setup, and adjust your strategy before continuing.

🟠 **Recurring CAPTCHA** – multiple in one session — often signal poor proxy quality or bot-like behavior detected by LinkedIn.

🟠 **Forced logout** or “Suspicious activity detected” alerts – something’s wrong. Some tools try to auto re-login, which can trigger even more red flags. GetSales avoids auto-login loops. Instead, we help you fix the root cause before LinkedIn escalates.

🟠 **Sudden drop in connection acceptance rate** – even if targeting is unchanged — red flag for shadowban. Shadowbans make your profile more sensitive to future triggers — meaning even small mistakes can escalate risk.

🛡️ 5 Safety Best Practices

Avoiding mistakes is only half the game — the other half is building safe, sustainable habits. These best practices won't just keep you out of trouble; they'll help you build credibility, improve engagement, and set up your outreach for long-term success.

1. Always **use an antidetect browser like GoLogin** to emulate a safe browser environment.
   Additionally, **warm up the session when possible** — this helps provide LinkedIn with more historical context.
2. **Use high-quality proxies**, for example Bright Data (used by GetSales), or 5G proxies that come with MirrorProfiles accounts (billed per traffic).
3. Minimize automation risk and ban rates by using the advanced solutions like GetSales — or by eliminating as many triggers as possible. **Our key protections** include: Server Schedule, single session protection, GoLogin integration, smart limits, warm-up, and ramp-up.
4. Follow best practices:

- Set up accounts properly
- Don't send spam or walls of text
- Don't include links
- Randomize limits
- Always warm up before launching campaigns

5. **If you're experiencing frequent logouts, it means something's wrong** — you need to identify and fix the root cause. GetSales can help you troubleshoot these issues quickly and provides full visibility into what's going wrong.

The authors:

Petr Kaliuzhny
Co-founder
GetSales

Frédéric D.
Co-founder
MirrorProfiles

Anton Herashchanka
Marketing Manager
GoLogin

This checklist was created by experts from three leading teams in LinkedIn growth, safety, and automation:

Peter Kaliuzhny, Co-Founder at **GetSales** — builder of one of the safest LinkedIn automation platforms in the market.

Frédéric Duhirel, Co-Founder at **MirrorProfiles** — expert in scaling and warming up LinkedIn accounts with real digital footprints.

Anton Herashchanka, Senior Marketing Manager at **GoLogin** — specialist in browser fingerprinting and antidetect tech for outreach safety.

Get Sales.io

The Safest LinkedIn Automation Tool

🚀 Want to scale like the big guys?

Top agencies already made the switch.
→ **Start safer outreach**