



Your Privacy. Restored.

Privacy Settings Guide

LinkedIn

LinkedIn has over 1 billion members and contains your professional history, connections, contact details, and location. In November 2025, LinkedIn expanded its AI training data policy globally – enabled by default for all members, with data processed before you opt out being irreversible.

What This Guide Covers

- Restricting contact information and profile visibility
- Controlling connections, activity, and search engine indexing
- Disabling the November 2025 AI training data opt-out (urgent)
- Managing ads, messaging permissions, and two-factor authentication

Why This Matters: LinkedIn Is the World's Largest Professional Intelligence Database

With over 1 billion members across 200+ countries, LinkedIn holds more verified professional data than any other platform. Your profile contains your employer, title, location, career history, connections, and contact details — a complete social engineering map. LinkedIn profiles are the #1 source used by fraudsters in executive impersonation and business email compromise attacks, which cost US businesses over \$2.9 billion in 2023 alone. Additionally, in November 2025, LinkedIn quietly expanded its AI model training policy to all global members and enabled it by default. Data already processed before you opt out cannot be reversed — making this the most time-sensitive setting in this guide.

What's at Risk If You Don't Act

- Your job title, employer, and career history used to craft highly convincing impersonation attacks
- Your connections list mapped to identify executives, assistants, and financial contacts at your firm
- Your contact information harvested by sales tools (Apollo, RocketReach, ZoomInfo all scrape LinkedIn)
- Your professional posts and messages used to train LinkedIn's AI models — including Copilot features
- Your location and work history used to build profiles on data broker platforms
- Profile visible in Google search results unless explicitly disabled

Your Legal Rights

- CCPA (California): Right to opt out of sale/sharing of personal data, right to know and delete — submit at linkedin.com/legal/privacy-policy
- GDPR (EU/UK): Right to object to processing for AI training (Article 21), right to erasure — contact LinkedIn's DPO at privacy@linkedin.com
- Virginia VCDPA, Colorado CPA, Texas TDPSA: Right to opt out of profiling and targeted advertising
- FTC complaint for deceptive practices: reportfraud.ftc.gov
- LinkedIn is subject to Irish DPC supervision for EU users — complaints: dataprotection.ie

Step-by-Step Privacy Configuration

Tip: Complete the initial setup using the desktop browser — it provides access to all settings in one place. The mobile app can be used for ongoing maintenance but has a more limited settings menu.

1 Access LinkedIn Privacy Settings

Navigate to LinkedIn's privacy and security settings:

- Click your profile photo in the top navigation bar.
- Select Settings & Privacy from the dropdown.
- You will see four tabs: Account preferences, Sign in & security, Visibility, and Data privacy.

2 Disable AI Training Data Use (November 2025 – Urgent)

Act Now: LinkedIn AI Training Is Enabled by Default Since November 2025

LinkedIn expanded its AI model training policy globally in November 2025. By default, your posts, articles, profile data, and interactions are used to train LinkedIn's AI systems including its Copilot and generative AI features. Data already processed before you opt out cannot be removed from trained models — opting out only prevents future use.

To opt out of AI training:

- Go to Settings & Privacy > Data privacy > Data for Generative AI Improvement.
- Toggle Use my data for training content creation AI models > OFF.
- Toggle Use my data for training AI models for content suggestions > OFF.

Note: LinkedIn may show this under 'Data for AI Improvement' or 'Generative AI' depending on your account region and app version. Search for 'AI' in the settings search bar if you cannot locate it.

3 Restrict Profile Information and Visibility

Part A — Hide Contact Information (Profile > Edit > Contact Info):

- Birthdate > Delete or set to Only you
- Email address > Only you or 1st connections only
- Phone number > Remove entirely or set to Only you

- Address > Remove street address; keep only city/state if needed
- Instant messaging handles > Remove all

Part B — Limit Name Information (Profile > Edit > Name):

- Remove middle name or initial to reduce identity exposure.
- Consider using first name + last initial for maximum privacy.
- Avoid nicknames that link to other social media accounts.

Part C — Public Profile Visibility (Settings > Visibility > Public profile):

- Change location to metropolitan area only — remove specific city and postal code.
- Edit your public profile URL to use a random string, not your real name.
- Under 'Choose what shows': uncheck all non-essential items. Keep only first name, last initial, and headline.

4 Control Visibility and Activity

Under Settings > Visibility, configure each setting:

- Profile viewing options > Private mode
- Who can see your email > Only you or 1st connections
- Who can see your connections > Only you
- Who can see your last name > 1st connections only
- Profile visibility off LinkedIn > No (prevents Google indexing)
- Share profile updates > Toggle OFF
- Notify connections of profile changes > Toggle OFF
- Show activity on profile > Toggle OFF
- 'People Also Viewed' and 'People You May Know' > Toggle OFF

Protect Your Connections List

Hiding your connections list is critical. Social engineers use visible connection networks to map your relationships and target your contacts with impersonation attacks. Set this to 'Only you' immediately.

5 Manage Advertising Data (Two-Profile System)

LinkedIn maintains two separate advertising data profiles — one based on your LinkedIn activity and one built from third-party data. Both must be configured.

Settings > Data privacy > Advertising data:

- Profile-based ads > Toggle OFF
- Interest-based ads > Toggle OFF
- Ads outside LinkedIn (LinkedIn Audience Network) > Toggle OFF

Settings > Data privacy > Third-party data for advertising:

- Toggle OFF Audience targeting based on inferred data
- Toggle OFF Lead generation forms pre-fill

Tip: The Advertising Data section is separate from AI training controls. Both must be disabled independently.

6 Manage Connections, Messaging, and Security

Connection and Messaging Settings:

- Who can send you invitations > Everyone (or restrict if preferred)
- Invitations from your network > Review message requests before accepting
- Who can send you messages > Connections only

Two-Factor Authentication (Settings > Sign in & security):

- Enable Two-step verification using an authenticator app (not SMS).
- Review Where you're signed in and remove unrecognized sessions.
- Under Active sessions, verify all devices are ones you own.

Passkeys available: LinkedIn supports passkeys as of 2024. Setting up a passkey (Settings > Sign in & security > Passkeys) is the most phishing-resistant authentication method available.

Verification Checklist

Setting	Configured Action
AI Training Opt-Out	Both AI training toggles > OFF (Data privacy tab)
Contact Info	Birthdate, phone, address removed; email > Only you
Public Profile	URL randomized; minimal info shown; location > metro only
Profile Viewing	Private mode enabled
Connections List	Visibility > Only you
Profile off LinkedIn	Disabled — profile hidden from Google/search engines
Activity Status	Share profile updates and activity > OFF
Ad Targeting (LinkedIn)	Profile-based and interest-based ads > OFF
Ad Targeting (3rd Party)	Audience targeting and lead forms > OFF
LinkedIn Audience Network	Ads outside LinkedIn > OFF
Messaging	Messages from connections only
Two-Factor Auth	Authenticator app enabled; SMS 2FA removed
Active Sessions	Reviewed; unrecognized sessions signed out

When Settings Are Not Honored

If LinkedIn does not honor your privacy settings or you believe your data is being processed contrary to your stated preferences:

1. LinkedIn Privacy Form: Submit a data request at [linkedin.com/help/linkedin/ask/ppg](https://www.linkedin.com/help/linkedin/ask/ppg).
2. GDPR Right to Object (EU/UK): Email LinkedIn's DPO at privacy@linkedin.com citing Article 21 of the GDPR.
3. FTC Complaint (US): reportfraud.ftc.gov
4. Irish Data Protection Commission (EU): dataprotection.ie — LinkedIn's lead EU supervisory authority.

Related guides: [Social Media: Facebook Privacy Settings Guide](#) · [Social Media: TikTok Privacy Settings Guide](#) · [Data Broker: ZoomInfo Opt-Out Guide](#) · [Education: AI Data Training Opt-Out Guide](#)



Need Help? VanishID Is Here for You.

Our team manages opt-outs and monitors for re-appearances on your behalf. Contact us if you run into any issues.

support@vanishid.com
vanishid.com