LinkedIn Security Enhancement: A Step-by-Step Guide

Take full control of your profile by managing visibility, privacy, and security settings. Fine-tune settings like who can see your profile and what they can see to protect your professional identity while ensuring your profile remains secure, private, and polished—perfect for making a powerful impression in your network.

🔑 The Basics: Passwords & 2FA

👁 **How to: Change your password**

☐ **Settings > Sign in & Security > Change Password:** Enter a strong password that combines letters, numbers, and symbols.

❓ **Why It Matters:**

- A strong, unique password helps protect your account from being easily hacked or compromised, especially if other accounts you own are breached.
- Consider using a password manager to securely store and manage your passwords.

👁 **How to: Ensure 2FA is enabled:**

☐ **Settings > Sign in & Security > Two-Step Verification:** Enable 2FA and choose an authentication method, such as SMS or an authenticator app.

Complete Setup: Follow the prompts to verify your identity and secure your account.

❓ **Why It Matters:** 2FA adds an additional layer of security by requiring a second form of verification, making it significantly harder for unauthorized users to access your account.

🛡 Review and Manage Privacy Settings

A. Control Profile Visibility

👁 **How to:**

☐ **Settings > Visibility > Review settings** on all these pages to ensure you're comfortable with the data you're sharing

1 . Visibility of your profile & network

- **Profile Viewing Options:** Allows you to choose how others see you when you view their profiles. You can display your name and headline, be semi-private with just your industry and title, or browse in complete anonymity (Private Mode).

☐ Page Visit Visibility: Determines whether the pages you visit can see that you have visited them. If set to "On," the page owners will know you visited.

☐ Edit Your Public Profile: Allows you to customize what people see when they view your LinkedIn profile outside of LinkedIn, such as through a search engine. You can adjust which sections of your profile are visible to the public.

☐ Who Can See or Download Your Email Address: Controls who in your network can view or download your email address. You can limit this to just connections or specific groups.

☐ Who Can See Your Connections: Determines who can view your connections list. If set to "On," your connections can see who else you are connected to.

☐ Who Can See Members You Follow: Limits visibility of the LinkedIn members you follow. If set to "Only visible to me," no one else can see who you follow.

☐ Who Can See Your Last Name: Controls the visibility of your last name on your profile, which can be useful for privacy or professional reasons.

☐ Representing Your Organizations and Interests: Determines whether you want to display your affiliations and interests publicly. If set to "On," these will be visible on your profile.

☐ Page Owners Exporting Your Data: Controls whether page owners can export your data, such as when you visit their page. Turning this "Off" restricts them from exporting your visit data.

☐ Profile Preview in Microsoft Applications: Controls whether your LinkedIn profile can be previewed in Microsoft applications, like Outlook. If set to "Off," your LinkedIn information won't be displayed in these apps.

Profile Discovery and Visibility Off LinkedIn:

- **Using Email Address:** Allows others to find your LinkedIn profile by searching with your email address. Setting it to "Anyone" means anyone with your email can find you.

- **Using Phone Number:** Controls whether people can discover your LinkedIn profile through your phone number. Setting it to "Nobody" restricts this feature completely.

2 . Visibility of your LinkedIn activity:

☐ Manage Active Status: Determines whether your connections and followers can see when you're online and active on LinkedIn.

☐ Share Profile Updates with Your Network: Controls whether your network is notified when you make changes to your profile, such as updating your job title or adding a new skill.

☐ Notify Connections When You're in the News: Determines whether LinkedIn will notify your connections when you're mentioned in the news or other online media.

☐ Mentions or Tags: Controls whether other LinkedIn members can mention or tag you in their posts.

☐ [Followers: Manages who can follow you and see your public updates. You can choose to allow everyone or just your connections to follow you.

❗ **Why It Matters:** Reviewing your visibility settings ensures you control who sees your LinkedIn activity and personal information, helping you protect your privacy and manage your professional image effectively.

🎯 Manage Data Sharing and Ads Preferences

How to:

☐ **Settings > Data Privacy > How LinkedIn Uses Your Data:** Review and adjust settings related to data sharing and ad targeting.

☐ **Third-Party Apps:** Review and revoke access to any third-party apps you no longer use or trust.

❓ Why It Matters: Managing your privacy settings helps you control who can see your information, reducing the risk of unwanted contact or data misuse. Limiting data sharing also decreases your exposure to targeted ads and potential data breaches.

🔒 Monitor Account Activity

How to: Regularly Check Account Access

☐ **Settings > Sign in & Security > Where You're Signed In:** Review all active sessions and sign out of any you don't recognize.

❓ Why It Matters: Regularly checking your account activity helps you detect and respond to any unauthorized access quickly, minimizing potential damage.

💬 Be Cautious with Connections and Messages

👁 **How to:**

- **Review Profiles Thoroughly:** Before accepting connection requests, ensure the profiles are legitimate and relevant to your network.
- **Avoid Suspicious Links:** Be cautious of messages containing links or attachments, especially from unknown connections.

❓ Why It Matters: Scammers and cybercriminals often use LinkedIn to target professionals. Being cautious with connections and messages reduces the risk of phishing attacks or malicious links.