

## Cheat sheet

	Goal	Recommendation
1	Secure your LinkedIn profile against social engineering.	<ul style="list-style-type: none"> <li>Ensure your Birthdate, Email, and Phone Number are not displayed in your Contact Information section. You can check this in <b>Profile</b> ⇒ <b>Edit (Pencil icon)</b> ⇒ <b>Contact Info</b>.</li> <li>To check if your email address is displayed, go to <b>Settings</b> ⇒ <b>Visibility</b> ⇒ <b>"Who can see your email address."</b></li> <li>Remove your middle name or middle initial if it's displayed in your profile name. To remove it, go to <b>Profile</b> ⇒ <b>Edit (Pencil icon)</b> ⇒ <b>Name</b>.</li> <li>Limit your location to your home country or home state. You can update this information at <b>Profile</b> ⇒ <b>Edit (Pencil icon)</b> ⇒ <b>Location</b>.</li> </ul>
2	Control who can see your information and updates.	<ul style="list-style-type: none"> <li>Navigate to <b>Settings</b> ⇒ <b>Visibility</b> to adjust who can view your profile, connections, and activity.</li> </ul>
3	Avoid accepting requests from unknown or suspicious individuals.	<ul style="list-style-type: none"> <li>Review profiles carefully before connecting and be wary of requests from individuals with incomplete profiles or those you don't recognize.</li> </ul>
4	Maintain a network of trusted connections.	<ul style="list-style-type: none"> <li>Periodically review your connections and remove irrelevant or suspicious ones. You can do this from your connections page.</li> </ul>
5	Create a password that is difficult to guess and not used in any other accounts.	<ul style="list-style-type: none"> <li>Use a combination of letters, numbers, and special characters. Consider using a password manager to generate and store a strong password.</li> </ul>
6	Add an extra layer of security by requiring a second form of verification.	<ul style="list-style-type: none"> <li>Go to <b>Settings</b> ⇒ <b>Sign in &amp; Security</b> ⇒ <b>Two-step verification</b> and follow the prompts to set it up.</li> </ul>
7	Ensure your security questions and answers are current and robust.	<ul style="list-style-type: none"> <li>Update your security questions under <b>Settings</b> ⇒ <b>Sign in &amp; Security</b> ⇒ <b>Change password</b>. Choose questions and answers that are difficult for others to guess.</li> </ul>
8	Limit access to your LinkedIn data by third-party applications.	<ul style="list-style-type: none"> <li>Check and manage app permissions under <b>Settings</b> ⇒ <b>Data Privacy</b> ⇒ <b>Permitted services</b>.</li> <li>Opt-out from allowing LinkedIn to feed your data to a Generative AI model by going to <b>Settings</b> ⇒ <b>Data Privacy</b> ⇒ <b>Data for Generative AI Improvement</b> and toggle <b>"Use my data for training content creation AI models"</b> Off.</li> </ul>
9	Stay informed about the latest security threats and best practices.	<ul style="list-style-type: none"> <li>Follow LinkedIn's security updates to stay current with new threats and preventative measures.</li> </ul>