What To Do If Your LinkedIn Was Compromised

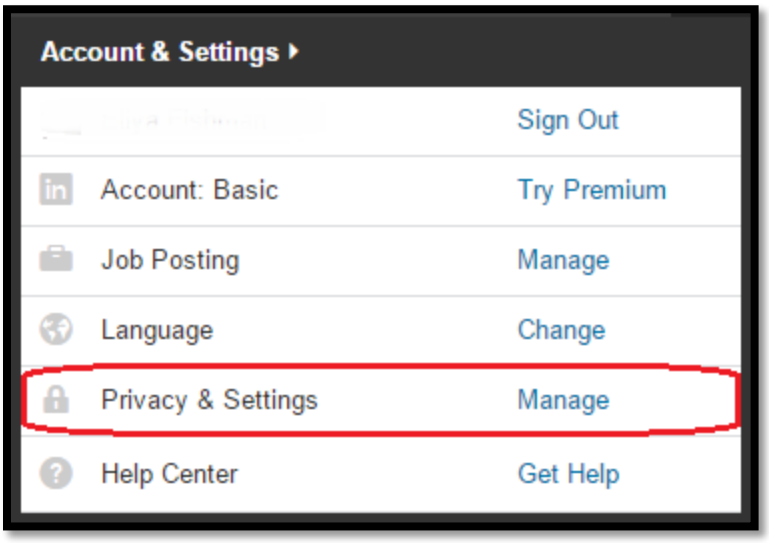
Step One: Check Your Email Account

Your email account is really the Fort Knox for hackers. If they can control your email account, then it means they can more easily access every other account you own. This is the first place you should check if you suspect something fishy.

Before you do anything else, clean out your email of compromising information.

Step Two: Change Your Password

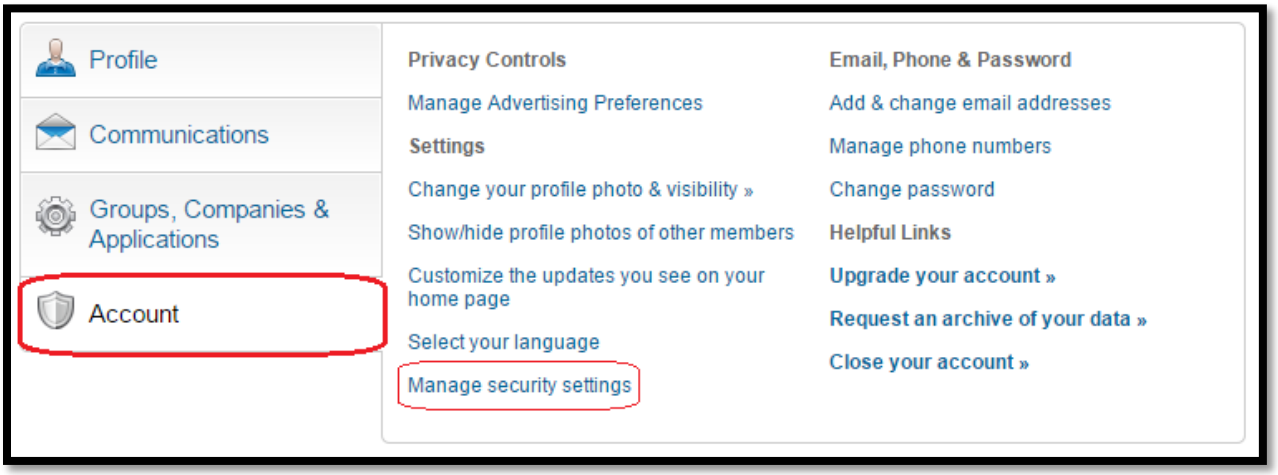
If someone has hacked into your account, that means they have your password. Immediately change this so you can regain control. You can do this on LinkedIn via the **Privacy & Settings** section of your **Account Settings**. Just run your mouse over your profile to find this menu. You'll hit **Change next to Password**, and this time, use a hack-proof password. Nothing obvious, and if you can throw in some numbers, uppercase letters, and special characters, it's all the better.

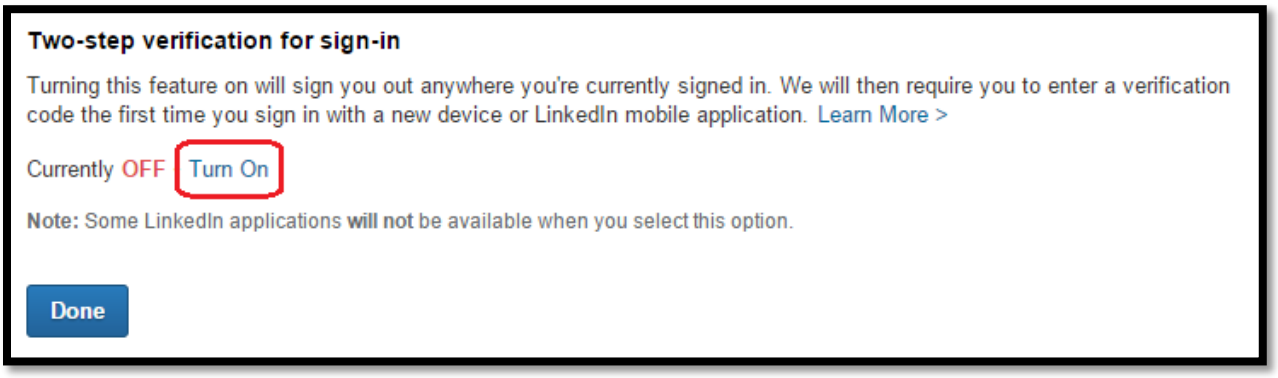


Step Three: Turn On Two-Step Verification

Two-step verification is the smartest way to keep hackers at bay. With two-step verification, LinkedIn will send a verification code straight to your phone whenever anyone attempts to log into your account from a new device. Without your smartphone, nobody is getting into your account.

Go to the Account tab under your profile, and click on Manage security settings. Turn on two-step verification, enter your mobile number, and verify the process.





Step Four: Contact LinkedIn

Contact LinkedIn at https://www.linkedin.com/help/linkedin/ask/TS-RHA if you can't access your account with your usual login information and notice changes being made to your connection list or profile. We will verify your ownership of the account to help you regain access.