LINKEDIN SMART CARD

MOBILE SETTINGS

South Dakota Consumer Protection Office of Attorney General

Dakota State University

SOCIAL NETWORK DOs and DON'Ts

- Only establish and maintain connections with people you know and trust. Review your connections often and block or unfollow people if needed.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share. Secure it!
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

MANAGING YOUR LINKEDIN PROFILE

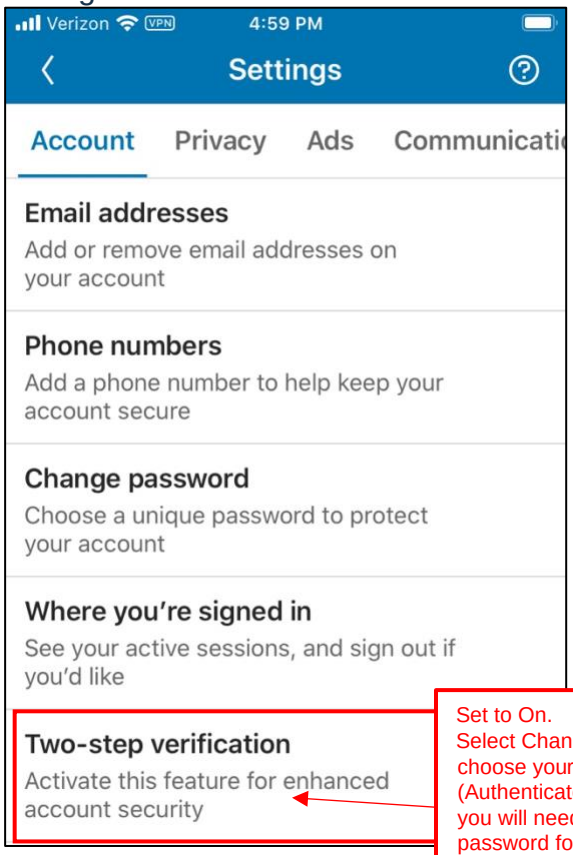
LinkedIn is a professional networking site whose users establish connections with co-workers, customers, business contacts, and potential employees and employers. Users post and share information about current and previous employment, education, military activities, specialties, and interests. To limit exposure of your personal information, you can review and manage who can view your profile and activities.

QUICK FACTS

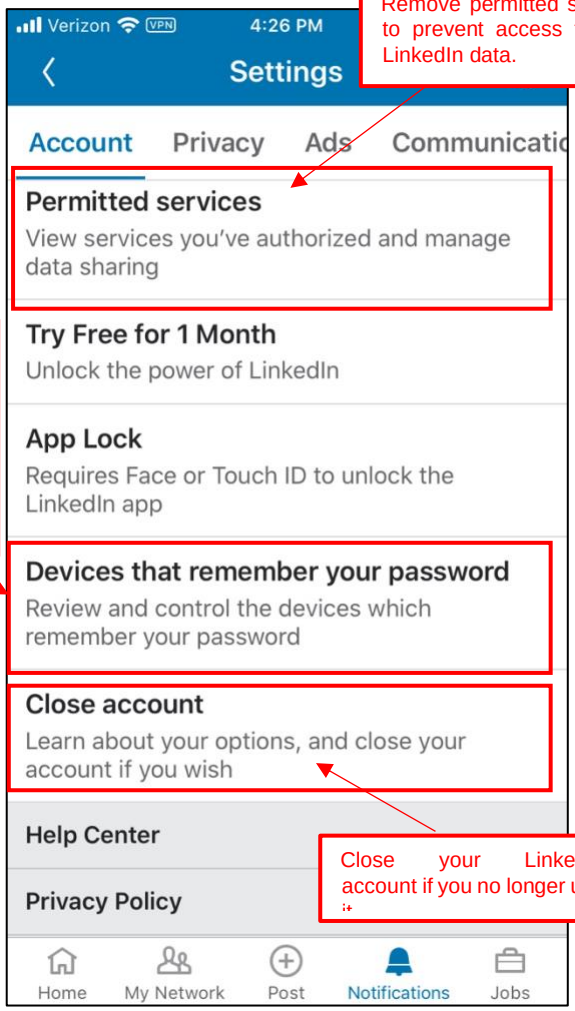
- There are over 500 million LinkedIn users around the world. 250 million monthly active users, only 3 million share contents on a weekly basis. Aside from the US, LinkedIn is widely adopted in India, Brazil, and the UK.
- Users tend to share information related to their careers or jobs as opposed to photographs from parties or social events.
- LinkedIn profiles tend to be more visible and searchable than social networks such as Facebook.
- Paid LinkedIn accounts have access to more information about other users, such as connections, than free accounts.
- The type of information users can see about each other depends on how closely they are connected (1st, 2nd, or 3rd degree).

MOBILE ACCOUNT SETTINGS

Access the LinkedIn app on your mobile device. Tap your profile picture on the top left area of the device. Tap **View Profile** under your name at the top, tap the gear icon at the top right.



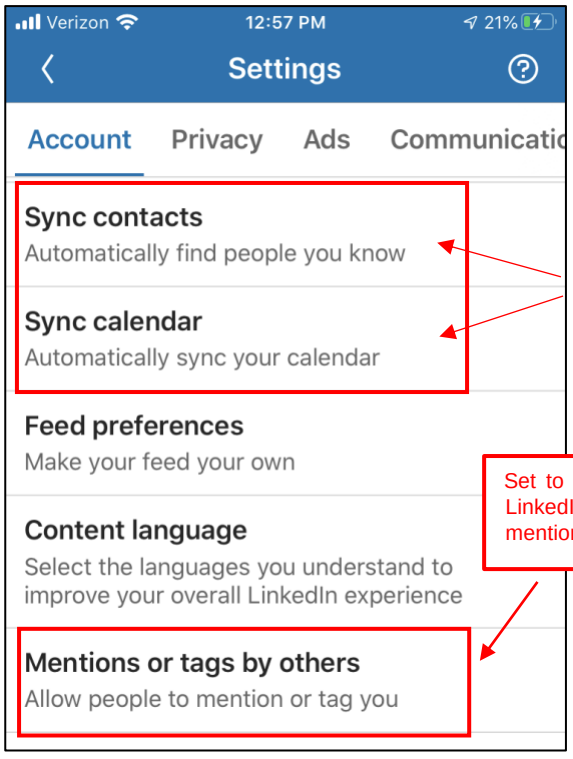
Set to On.
Select Change Verification Method and choose your verification method (Authenticator App or Phone Number – you will need to enter your LinkedIn password for either option).



Remove permitted services to prevent access to your LinkedIn data.

Review devices that remember your password – remove any you do not recognize. After removing unknown devices change your password to ensure no one else is signed in to your account.

Close your LinkedIn account if you no longer use it.

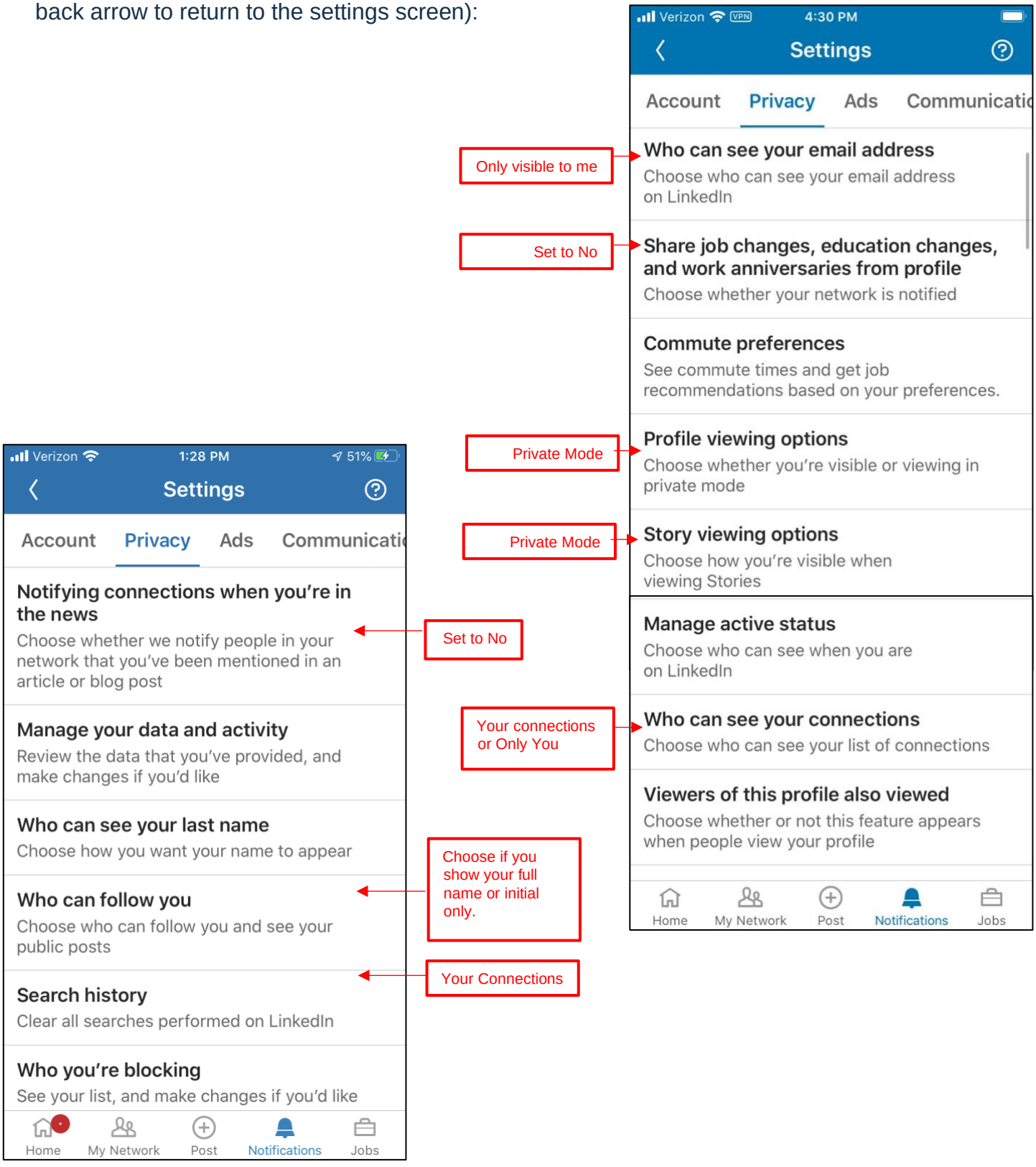


Set both to No to limit LinkedIn's access to your contacts and calendar.

Set to No to prevent other LinkedIn users from mentioning or tagging you.

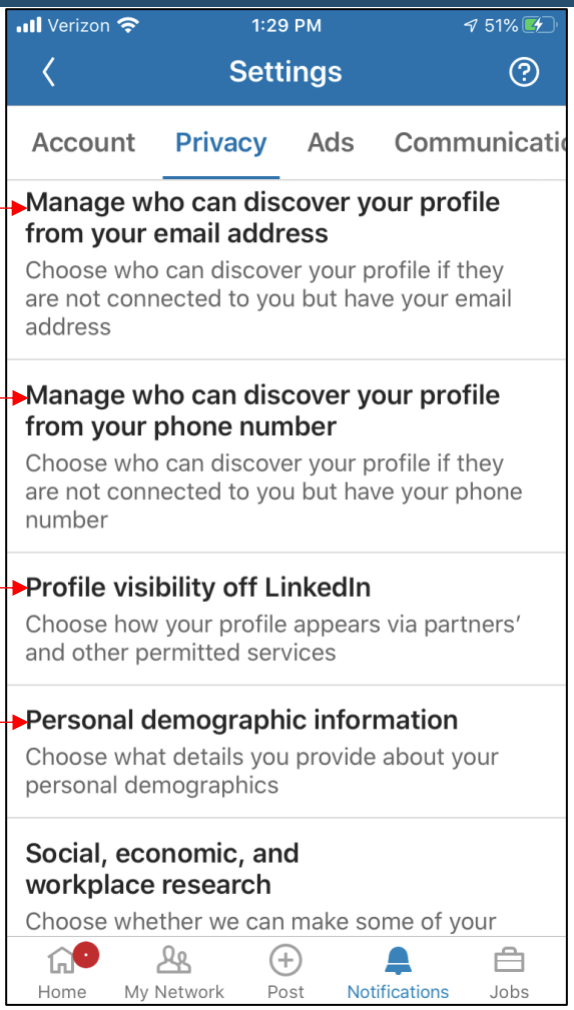
MOBILE PRIVACY SETTINGS

Select **Privacy**, for each option use the following settings shown in red (after each option select the back arrow to return to the settings screen):



MOBILE PRIVACY SETTINGS - continued

- **Two-step verification** – *Set Up for additional security – enter your LinkedIn password and select Send code*

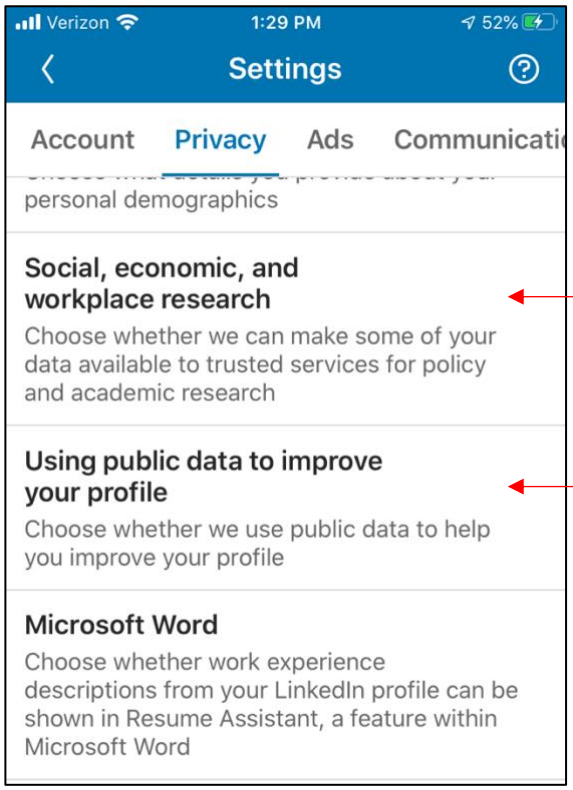


Nobody

Nobody

Set to No

Choose what personal information you want LinkedIn to have.

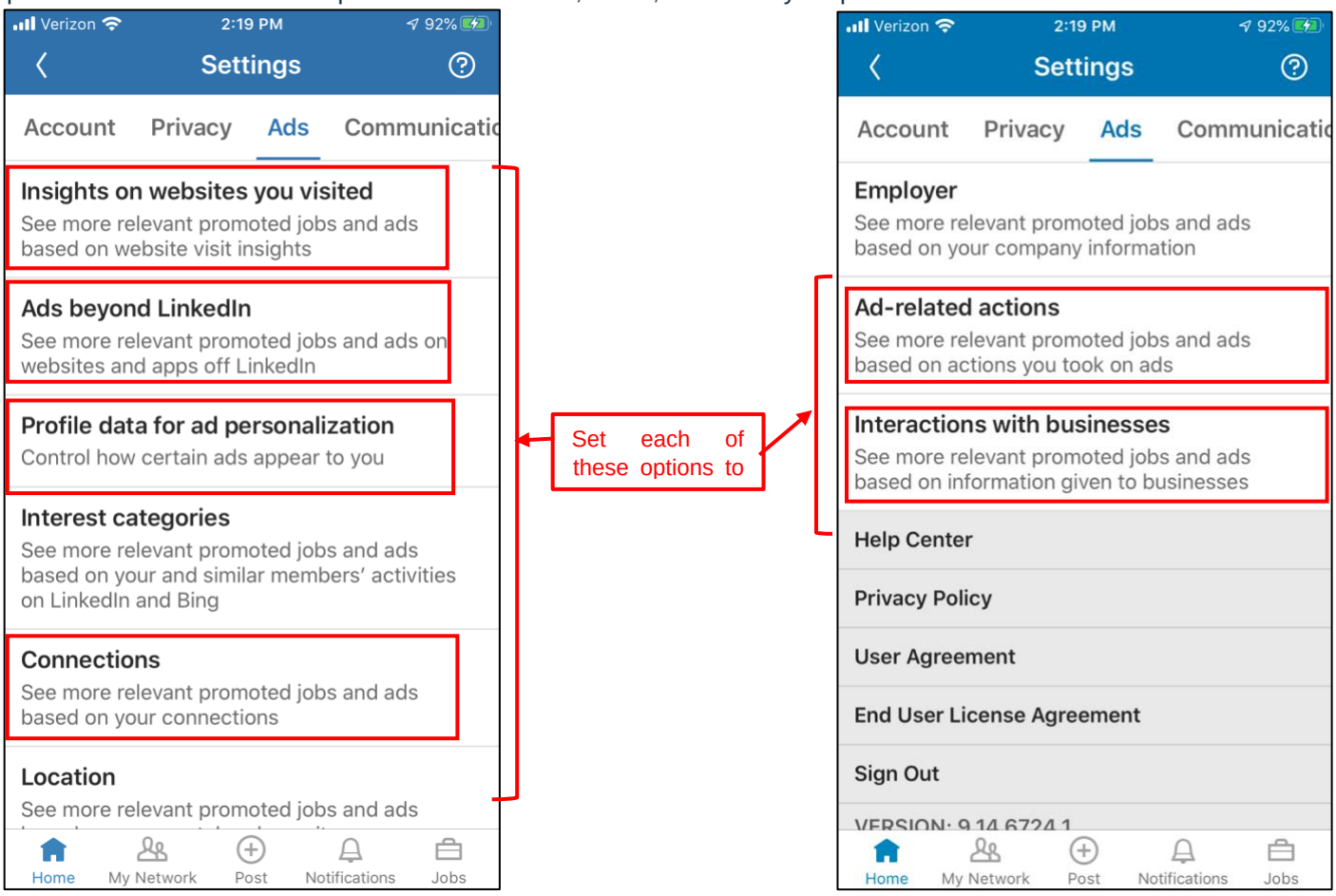


Set to No

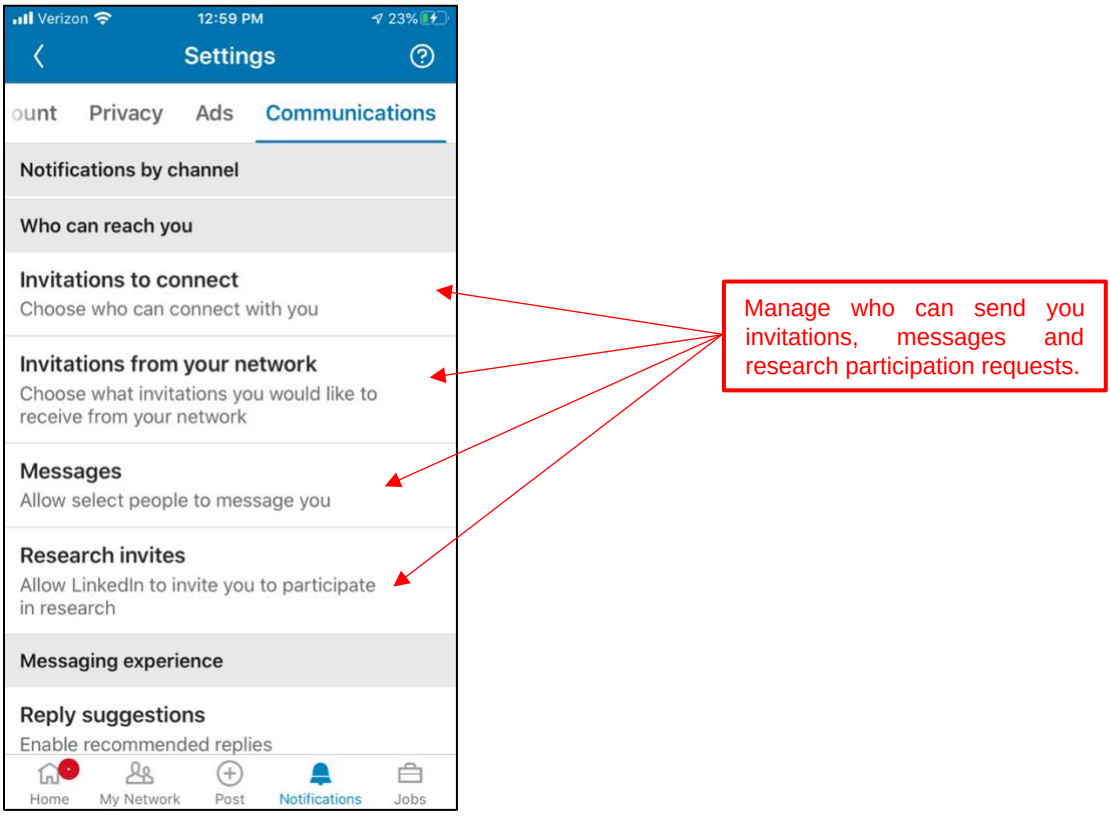
Set to No

MOBILE AD SETTINGS

Third-party applications and services can access your personal information once you authorize them in your settings. Limit the use of applications to ensure that third parties cannot collect, share, or misuse your personal information.



MOBILE COMMUNICATIONS SETTINGS



PASSWORD RECOMMENDATIONS

- Minimum of 8 characters is recommended.
- Use a combination of upper and lowercase letters, numbers and symbols/punctuation marks.
- Should not contain your name, username, phone number, birthday, pets' names or other personal information.
- Should be unique to each app or website you use - use a password manager to keep track of multiple passwords.
- Don't use common words (dictionary, iloveyou, password) or series of letters (qwerty, abcd1234).
- Using a longer passphrase or series of words may be easier to remember and more secure.

USEFUL LINKS

A Parent's Guide to Internet Safety
www.fbi.gov/stats-services/publications/parent-guide

Wired Kids
www.wiredkids.org

Microsoft Safety & Security
https://support.microsoft.com/en-us/help/4091455/windows-protect-privacy-internet

OnGuard Online
https://www.consumer.ftc.gov/features/feature-0038-onguardonline

LinkedIn
https://www.linkedin.com/help/linkedin/answer/66/managing-your-account-and-privacy-settings-overview?lang=en

Last reviewed/edited: 5/4/2020

South Dakota Consumer Protection Office of Attorney General

Dakota State University