FITBIT SMART CARD

MOBILE SETTINGS

South Dakota Consumer Protection
Office of Attorney General

Dakota State University

SOCIAL NETWORK DOs and DON'Ts

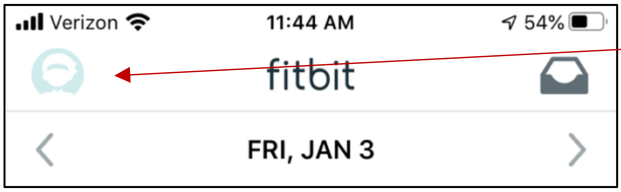
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; 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 FITBIT ACCOUNT

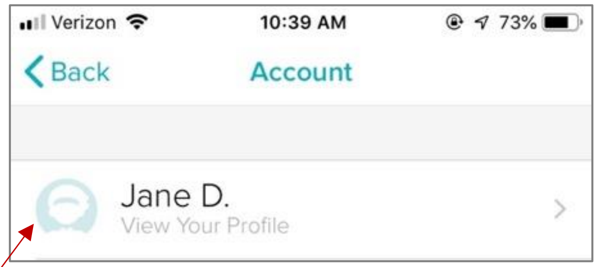
Keep your Fitbit software and device updated to ensure you receive the latest security updates.

PROTECT YOUR FITBIT INFORMATION

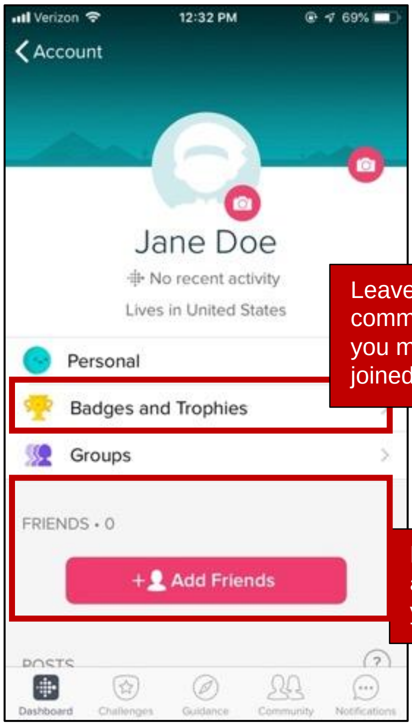
Edit your profile. Adjust your profile settings to show minimal personal information such as setting your Display Name to a username rather than actual name.



Tap to enter settings



Tap to access user profile.

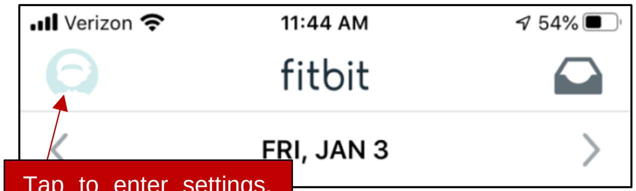


Leave any community Groups you may have joined.

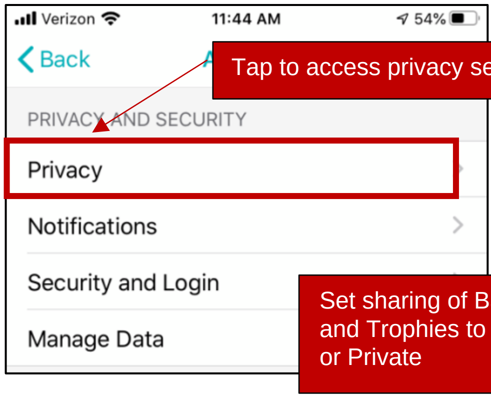
Remove or block any "friends" that you do not know.

PRIVACY

Make all your personal stats private.



Tap to enter settings. Scroll down on account screen to find Privacy and Security.

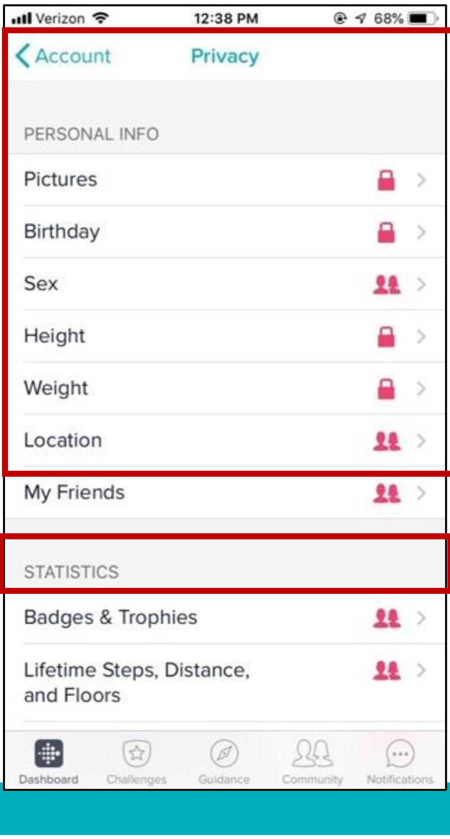


PRIVACY AND SECURITY

- Privacy
- Notifications
- Security and Login
- Manage Data

Tap to access privacy settings.

Set sharing of Badges and Trophies to Friends or Private



PERSONAL INFO	
Pictures	🔒
Birthday	🔒
Sex	👥
Height	🔒
Weight	🔒
Location	👥
My Friends	👥
STATISTICS	
Badges & Trophies	👥
Lifetime Steps, Distance, and Floors	👥

Set sharing of personal info to either Friends or Private

PASSWORD RECOMMENDATIONS

- Minimum of 8 characters is recommended.
- Use a combination of upper and lowercase letters, numbers and symbols/punctuation marks.
- Enable two-factor authentication when available.
- 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

Fitbit Help
https://help.fitbit.com/?l=en_US&c=Topics%3AAccount_Settings

Last edited/revised: 5/4/2020

South Dakota CONSUMER PROTECTION OFFICE OF ATTORNEY GENERAL

DAKOTA STATE UNIVERSITY