COMPASS
COMMUNITY CREDIT UNION
Guiding you to better banking

Stopping fraud on the go

The convenience of mobile banking allows you to handle your banking on the go. Unfortunately, mobile identity theft is also on the rise. Users should protect their privacy and their financial security by following these do's and don'ts.

Do:

- Use strong alphanumeric passwords and change them regularly
- Log out when you exit a social networking site like Facebook
- Install and maintain up to date industry trusted antivirus and spyware software
- Lock your mobile device with a password, so information can't be accessed if it's lost or stolen
- Check out the reviews of an app before you download it
- Let your financial institution (us!) know if you lose your phone or change your phone number
- Monitor your accounts and credit report frequently for fraudulent or suspicious transactions

Don't:

- Access financial accounts when using free public Wi-Fi, unless you've installed encryption
- Put personal or account information in an unencrypted text or email
- Store sensitive information such as account numbers in your mobile
- Use the same password for multiple accounts
- Share your birthdate, email address, or personal details in a social media profile visible to anyone
- Click on pop-ups or open attachments from dubious senders (anything you didn't request yourself is suspicious)