Nichole Hasley
Marketing, Anaconda Branch

Mobile Banking Safety.

Like with any other app, you first need to make sure you are downloading your app from your devices app store. Banking apps have come along way in the form of securities such as fingerprint and face recognition and multi-factor authentications (MFA). MFA is a multi-step account login process allowing users to enter additional information to secure a log in. This typically is a code that is sent to the users phone or email the user choses at time of set up. NEVER share this code with anyone. Banks and credit unions use high end encrypted technologies that help safeguard your information. Additional safeguards you should always be cautious of is avoiding public wifi. Only use your carriers cell service or hotspot. Make sure you use a pass phrase or a complex password and never right it down where someone could easily find it. Changing out your password often can also provide you with an extra layer of protection.

More and more, we see text messagese sent with links claiming to be your instituition and luring you to click the link to learn more to solve a problem that you may or may not have encountered. If you were not expecting a text message, you should always reach out to your instituion FIRST before clicking any links, no matter how legitimate the message may appear. Your instituion will let you know if the message is real and if you should take further action.