Imagine one day finding out that someone has been posting ads on your Facebook account. You go to sign into your account and find that someone has changed your password. Tough luck looks like someone got your password in one way or another and gained access to your account. This is a real situation that my family has been put through. However, if I were to have had an MFA this would have never happened. At the first attempt of this hacker logging in you would have been given a notification and been prompted as to if this person was you or not.

MFA stands for multiple-factor authentication and it is a safeguard against situations like this. MFA is essentially a second lock you can put on an account that directly contacts you whenever someone tries logging in including yourself. This lock works in a two-step verification process that requires someone to enter a password and then approve the loggin' through an app. These MFAs are gonna ask for proof of identity whether it be through a password, thumbprint, or text. This process makes it significantly harder for hackers to access your account even if they have your password. The average experience with an MFA would look something like this. You sign into your account by entering your username and password. You enter everything correctly and now you are prompted by a notification from the MFA. You then navigate to whatever MFA platform you are using and verify that the person signing in is you. You would then be allowed access to your account from there.

Now MFA can still have security breaches but not in the way that we described in the Facebook example. For one MFA are very unlikely to be targeted for cyber attacks. If someone were to gain control of your MFA they would still need access to your accounts to use it correctly, and as you can have multiple MFAs for different websites and accounts you can create a maze with your apps. Sadly the biggest issues are caused by the account owners. This case usually involves the hacker requesting access to the account and the user letting them in. This is usually just a case of people being pestered by notifications and giving into them and allowing the hackers access. Never give anyone access to your account if the person signing in is not you. Other than that though it is seen as a foolhardy plan for hackers to target your MFA.

There are plenty of great examples of MFA being used by people now. UTSA even uses an MFA that is called DUO. This app uses notifications, passwords, and text as a way to keep school accounts like blackboards and emails protected. A big company that uses an MFA is a steam. Steam is a platform that allows people to buy and play video games and has become the main platform for people to buy games. Steam has made an MFA called Steam Guard that protects the sign-in to your accounts. Steam Guard uses randomly generated passwords as a method to keep your accounts safe. This password resets every 30 seconds and is made of 8 digits ranging from numbers letters and symbols. Whenever people need to sign in the password is required to be entered to give access. These Steam accounts hold a lot of value as games are stored on them as well as credit card info. If someone were to gain access to this account things could be catastrophic. I fell for a phishing scam once where I gave people access to a Steam account, but because I had Steam guard the attackers were not allowed in the account. In a case where I used an account that had no guard, the password changed instantly and I could no longer sign in. Learn our mistakes and get an MFA now!