As we head into the holidays, we would like to remind our members to ensure that you are using the most secure settings available on your online banking. Over the holiday's cybercriminals more frequently attack financial institutions and the first line of defense in the event of an attack is a strong password. These attacks are typically brute force attacks, which is when a cybercriminal uses automated tools to attempt thousands of combinations of login IDs and passwords. The goal of these attacks is to gain access to your account and transfer funds out. We would like to urge all of our members to use the longest possible password and setup login alerts to notify you when your account is accessed.

What is a strong password?

There are two ways to increase passwords:

- Increase length
- Increase complexity

The longer your password is, the more secure it becomes, and we strongly recommend using the longest possible password because of this. You should avoid an easy to guess password like the examples below:

- 12345
- 121212
- 87654321
- 69696969
- 000000

In addition to strong passwords, we also provide a robust alert system to keep you updated on your account activity. Both password settings and alerts are accessed through the menu on the left side of online banking. Passwords settings are under Profile and Preferences while alert settings are under Messages and Alerts. Please contact us at 780-929-8561, through MemberDirect or come in branch and we would be more than happy to help you with better securing your account.