Online and Mobile Banking Tips

There are precautionary steps you can take to maintain and protect your information online:

- Make sure to memorize your User ID and Password. Make sure no one watches you enter your User ID or Password information on the computer.
- If you cannot remember this information, write it down and store it in a secure location.
- Never allow your Internet browser to store your information. Many browsers ask you to save this information so you don't have to type it every time you use an online service. Although useful, storing personal access codes in this manner is a security risk. This is even more important if you use mobile banking.
- Avoid storing your access codes or any personal information like Passwords or social security numbers on your mobile device.
- Password protect your mobile device and lock it when you are not using it.
- Change your Password from time to time.
- Use a unique Password that doesn't contain personal information or is easy to guess. Do not choose a Password too similar to your User ID.
- When you are finished conducting business online, make sure to log off instead of simply closing your browser. This will ensure your secure session has been closed.
- Be aware, particularly when using public computers, that viruses and software exist which record keystroke information and could compromise your online security.
- If you should ever receive an email asking for account or password information that claims to be from Princeton Federal Credit Union please contact us immediately by dialing 609.945.6200.
- Run routine audits on your computer and mobile device to ensure they are free of viruses.

- Monitor your account regularly and report any suspicious activity to Princeton Federal Credit Union immediately by dialing 609.945.6200.