ONLINE BANKING PASSWORD/SECURITY BEST PRACTICES

Passwords

- Choose longer passwords, such as a phrase rather than a single word.
- Use a mix of upper and lowercase letters.
- Include numbers and special characters.
- Avoid common sequences, such as “1234.”
- Avoid using personal information, such as your name, pets’ names, date of birth, etc.
- Avoid using an automatic login feature that stores your username and password.
- Do not use the same password for multiple online applications.
- Change your password frequently.
- Never share your username and password with third-party providers.

Security

- Do not use public or other unsecured computers for logging into Online Banking.
- Do not login to online banking from public Wi-Fi, while it may be convenient to stay connected on the go, you cannot count on it to be secure. Some security risks posed by public Wi-Fi include:
    - Man-in-the-middle attacks, in which hackers can electronically “eavesdrop” on your banking and other online activity
    - Data transmissions over unencrypted networks
    - Malicious hotspots
    - Malware and spyware
- Review account balances and transaction details regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to Sugar River Bank
- Sign up for balance and transaction alerts by email, text, or both.
- Be wary of Phishing scams - we will never call or email you requesting your username, password,Personal Identification Number (PIN), or answers to your security questions.
- If attachments and links in email are unexpected or suspicious for any reason, do not click on them.
- Keep anti-virus/anti-malware software installed and up to date on computers accessing online banking.
- Never leave devices unattended unless they are locked so no one else can use them.
- Protect your mobile device by:
    - Adding a PIN or Touch/FaceID to unlock
    - Only install apps from trusted sources such as Apple AppStore or Google Play
    - Keep the operating system up to date
    - Avoid transmitting or storing personal information on the device
    - Use Apple’s Find my iPhone or the Android Device Manager tools to help prevent loss or theft

Use of Cookies

What is a cookie?

Cookies are text files with small pieces of data that are used to identify your computer as you use a browser. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience.

Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer. When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you.

How do we use cookies?

We collect cookies from our users for various reasons, not least to track our own performance – but also to let us serve you content tailored to your own specifications, hopefully improving your overall experience of the website. Amongst other things, the cookies we use allow users to register a device and skip the 2 factor authentication step after the first time login.

What types of cookies do we use?

There are two cookie types used:

- Persistent cookies remain on a user's device for a set period of time specified in the cookie. They are activated each time that the user visits the website that created that particular cookie.
- Session cookies are temporary. They allow website operators to link the actions of a user during a browser session. A browser session starts when a user opens the browser window and finishes when they close the browser window. Once you close the browser, all session cookies are deleted.

How do I remove cookies?

Every major browser makes it easy to view and delete the cookies stored by it. However, the process varies from one browser to the next.

In general, you will want to open the browser settings and look for the privacy or security section. Next, look for an option that allows you to view the cookies stored by your browser. When viewing individual cookies, you will be provided the option to delete any cookies you wish to remove from your browser. You should also find an option to easily delete all cookies if you wish to do so.

Please keep in mind that deleting cookies for our website will remove the device registrationand require you to enter the 2-factor authentication code upon each login.