Five Tips for Maintaining Your Security When Banking Online

In today's world being able to access your banking information whenever and wherever is key. That's why so many Americans bank online. In fact, according to the American Bankers Association Journal, approximately 70 percent of Americans say they most often access their bank accounts via online and mobile channels. While online banking is no doubt convenient, there are risks involved, and given October is National Cybersecurity Awareness Month, there is no better time than now to reinforce some best practices to help you maintain your security when banking online.

Here are five tips to help stay safe.

1. **Protect Your Passwords.** In addition to creating a strong password, it's important to *remember* the password. Rather than creating a written password list which can be stolen or misplaced, use a password manager app that will store all of your passwords. This only requires that you remember your password for the password manager. Additionally, if you store your banking data on your computer or mobile devices, make sure they are password protected. This will make it much more difficult for a thief to access your data if your computer or phone are ever lost or stolen.

2. **Update Your Software.** Computer and mobile device manufacturers update their software regularly, not only with new features, but with enhanced security. Make sure you initiate these updates on your computer and mobile device. Additionally, don't forget to maintain your antivirus software and always make sure your bank's app is updated on your mobile device.

3. **Stay Protected While You are Connected.** If you access your bank data from an unsecured network, your data can be compromised. Connecting to public Wi-Fi can expose your personal information. If you can't wait until you get home to connect to your home network, we suggest you use the bank app on your phone while you are connected to your mobile provider.

4. **Never Share Your Bank or Personal Information.** Beware of hackers and identity thieves who use phishing scams to access your personal or banking information. These scams include creating fake websites to look like your bank or emails or phone calls that appear legitimate but are not. Your bank will never send you a request for your personal or banking information. Always be vigilant. If an email or phone call sparks suspicion, call your bank directly, using the contact information you already have.

5. **Use Alerts to Monitor Banking Activity.** You can set up alerts in online banking to help spot unusual banking activity. Additionally, you can secure your SB One Bank debit card by using Card Valet which allows you to control when, where and how your card is used.

Online security is a big issue. Don't take it lightly. Visit the National Cybersecurity Alliance website here for further information and guidance.