

Bank of Utah Secure Banking

Security is a priority at Bank of Utah. Whether you're accessing your accounts on your desktop computer, laptop, tablet or phone, we use specialized software and other technologies to keep the information you've entrusted to us confidential and safe.

How Do We Protect Your Information Online and in the Mobile App?



Technology

We secure your online banking connection with Secure Socket Layer (SSL) technology, which encrypts your personal information before it even leaves your computer.



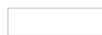
Browsers

We require the use of a secured, 128-bit browser (the strongest encryption available), such as Chrome, Safari, Firefox and Edge, to log in to your account.



Automatic Log Out

We automatically sign you out of your banking session after 10 minutes. To stay safe, it is best to log off and close your browser after completing your business.



Limited Log In Attempts

We temporarily disable your account after too many failed log-in attempts. If your account has been disabled, you must contact the bank to regain access.



Authentication

We require you to verify your identity each time you log in on an unregistered device, by using multifactor authentication.



Alerts

We send automatic alerts when we receive instructions to make important changes to your account, such as changes to your name, address, username and password.

How Can You Take Extra Measures to Ensure Your Safety Online?

1. **Keep your passwords strong and unique.** Do not reuse passwords. The longer and more complex the password or passphrase, the harder it is to hack. Learn how to [create a strong password and passphrase](#).
2. **Change your security settings to enable multifactor authentication for all your accounts.** Multifactor authentication requires multiple forms of verification, like a text or email with a code, to prove your identity.
3. **Don't use free, public Wi-Fi** when logging in to any financial portal.
4. **Be wary of links or attachments in emails**, especially if you're not expecting the email or it comes from someone you don't know.
5. **Only download apps from the authorized app store on your mobile device** (AppStore, Microsoft Store, Google Play, etc.).
6. **Keep your computer software up to date**, and always make sure to have an anti-virus, anti-spyware and firewall installed.
7. **Set up alerts for your accounts.** In online or mobile banking, go to the Settings menu, click Alerts, and choose the ones you'd like to receive.
8. **Take control with CardValet**, a free app for Bank of Utah customers that will notify you when your Bank of Utah debit card is used, let you restrict transactions to a certain area, and allow you to lock and unlock your card.

Get more tools and information to keep you safe.

[Visit Our Fraud Protection Resource Library](#)

Have Questions About How to Bank Securely?

[Contact Us](#)

Digital Protection

- [Online Best Practices](#)
- [Creating Strong and Unique Passwords for Each Account](#)
- [Kids Online Safety](#)
- [Social Media Scams](#)