

About Infinity Credit Union Digital Banking Security



The security of your personal information is of the utmost importance to Infinity Credit Union. We have state-of-the-art systems to secure our computer servers and networks and several additional layers of security to ensure your personal and account information remains safe and secure. Listed below you will find information about some of the measures we have in place. Of course, there are details we cannot provide to maintain the integrity of our security systems.

Measure	Description
24/7 Monitoring	<ul style="list-style-type: none"> All Online and Mobile referred to as Digital Banking hardware and software systems are continually monitored to proactively prevent issues from arising. An online enrollment is required before the account can be accessed via Digital Banking. The enrollment process must pass several layers of authentication before it can be completed.
Account # and Password	<ul style="list-style-type: none"> We require that an account and password be used whenever the account is accessed through Digital Banking. Your online password can be managed from Digital Banking. We restrict the use of easily guessed passwords for your own protection. A series of invalid logon attempts will block the account from further online access, until further verification is completed. Instructions will display on the screen in the event this occurs on your account. We maintain detailed information on the failure attempts made on accounts.
Encryption/TLS	<ul style="list-style-type: none"> Our web servers are equipped with a Digital Secure Certificate, encrypting or scrambling information sent to and from the server via Transport Layer Security (TLS) technology. TLS is the leading security protocol on the Internet.
Firewalls	<ul style="list-style-type: none"> Our network is protected from outside intrusion by state-of-the-art redundant and load-balanced firewalls. These secure mechanisms control and prevent non-authorized access to our internal systems.
Internet Client Browser	<ul style="list-style-type: none"> We require Internet browsers that support 128-bit encryption, the strongest commercially available protection. This encodes and encrypts all information traveling between your computer and ours. We also ask that you use the latest version of Chrome, Internet Explorer, Edge or Safari, since many browser security issues have been addressed in the most recent versions of these browsers. In addition, you should check with your browser provider on a regular basis to install any recent security patches or updates. You can easily determine if a site is secure. On secure sites, a padlock will be displayed on the right of your browser's status bar, indicating the site is using a digital secure certificate and TLS is in place. See Encryption/TLS below for further details.
Intrusion Detection Systems	<ul style="list-style-type: none"> This mechanism scans network traffic for any possible malicious attacks to our systems.
Second Authentication	<ul style="list-style-type: none"> After you log in to Digital Banking using your usual account number and password, you may be greeted with a security page. This page will prompt you to select and provide answers to at least four security questions. The information you enter will be stored in Digital Banking for future use in helping to confirm your identity. This additional level of authentication will ensure that Digital Banking continues to be an extremely safe and reliable system for a long time to come.
Secure emails	<ul style="list-style-type: none"> Our Digital Banking platform allows you to submit secure e-mail to our Member Service Team. When our Member Service Team responds, they will remove any sensitive data from your original e-mail before they reply. An example of this e-mail form can be accessed by clicking on the "Contact Us" link found on the top navigation menu when inside Digital Banking
Server Logs	<ul style="list-style-type: none"> For your protection we record all online activity in detailed logs. This allows us to investigate problems. Logs are also monitored frequently to identify unusual activity.
Session Timeout	<ul style="list-style-type: none"> A session timeout will automatically terminate your online session. A time out occurs when the Digital Banking session is idle or inactive for a period of time.
Systems Security Audits	<ul style="list-style-type: none"> Our systems are frequently audited by outside experts to identify and rectify any vulnerabilities.

202 Larrabee Rd Westbrook, ME 04092
(207) 854 – 6000 or (800) 499-8401 or email operations@infinitycu.com