



How we protect you

Encryption

The privacy of communications between you (your browser) and our servers is ensured via encryption. Encryption scrambles messages exchanged between your browser and our online banking server.

Password Complexity

It is important to verify that only authorized persons log into online banking. This is achieved by verifying your password. When you submit your password, it is compared with the password we have stored in our secure data center. We allow you to enter your password incorrectly a limited number of times; too many incorrect passwords will result in the locking of your online banking account until you call us to reinitialize the account. We monitor and record "bad-login" attempts to detect any suspicious activity (i.e. someone trying to guess your password).

Enhanced Login Security

This feature improves the security of your Internet banking account. When you enroll as an online customer of Hingham Savings, a unique, secure device ID will be placed in the browser of your computer. We will check for both your password and your computer to validate your login. If you login from a computer we don't recognize, we will ask you more questions to validate your identity.

You play a crucial role in preventing others from logging on to your account. Never use easy-to-guess passwords. Examples:

Birth dates

First names

Pet names

Addresses

Phone numbers

Social Security numbers

Never reveal your password to another person. You should periodically change your password in the User Option section of Internet Banking.

Secure Architecture

The computers storing your actual account information are not linked directly to the Internet.

Transactions initiated through the Internet are received by online banking Web servers.

These servers route your transaction through firewall servers.

Firewall servers act as a traffic cop between segments of our online banking network used to store information, and the public Internet.

This configuration isolates the publicly accessible Web servers from data stored on our online banking servers and ensures only authorized requests are processed. Various access control mechanisms, including intrusion detection and anti-virus, monitor for and protect our systems from potential malicious activity. Additionally, our online banking servers are fault-tolerant, and provide for uninterrupted access, even in the event of various types of failures.

Online Banking Features that promote Security:

We provide a number of additional security features in online banking to help protect you:

Timeout: This prevents curious persons from continuing your online banking session if you left your PC unattended without logging out. You may set the timeout period in online banking's User Options screen. We recommend that you always sign off (log out) when done banking online.

Check Images: View an exact facsimile of your check transactions online to help prevent fraud.

Alerts: Check clear alerts, payment alerts, and balance alerts are financial tools we provide to help you to monitor your accounts more actively and to detect suspicious activity more easily.