Security Controls

Digital Banking provides Internet Banking and Mobile Banking channel access for delivery of information to our customers. These channels must have controls in place to limit exposure to unauthorized access of account information. Century Bank works with our vendors to develop a secure infrastructure to minimize exposure to unauthorized access of account information. Controls to limit exposure and unauthorized access to account information can be identified in three primary areas: Access, Network, and Processing.

Access Controls

Cookies are small text files placed on the user's computer by a web site. Internet Banking, like many other commercial web sites, uses a technology called "cookies" to provide tailored information from the web site. There are two types of cookies: persistent cookies and temporary or session cookies.

Century Bank's Internet Banking sites use session cookies to assist in securing activities and to enhance the performance of our web sites. Session cookies are used for authentication purposes. Once a user logs in to a web site, the browser receives a session cookie that has a time stamp on it. As the end user moves around a web site, the browser submits the session cookie whenever the browser requires a private web page. This is how the site knows that the person who logged in is the same person requesting the private pages.

Internet Banking persistent cookies contain an encryption key in the cookie that must match the encryption key on the database at the web host location in order to skip the security questions previously entered when creating the password.

Century Bank uses the "device fingerprint" option with regard to the "Remember this device" feature functions. Century Bank believes the "device fingerprint" is the most advanced method available because it does not require the use of a persistent cookie. The fingerprint is a proprietary hash created from various hardware and software components that can uniquely identify a particular device for digital banking services, creating a known device. This allows the device to move from one IP to another and still function properly. This option allows for the highest level of security and usability.

Additionally, the end user's computer expires based on the "Days Until Security Cookie Expiration". The numeric value is the number of days the security cookie is valid. After that time, the computer is required to be registered again.

In addition to the authentication in place for Digital Banking, the Mobile Banking app offers specific validation options. The option of "PIN" allows a user to create a 4-digit code for login on a known app device. The option of "biometrics" permits fingerprint access in place of credentials on a known device. SMS/text banking is also available for client access. This service authenticates based on phone number and returns select information upon request.

Enrollment - First-Time User Setup

The internet banking system will be able to randomly generate a 20-character setup key based on a unique ID for the customer. This setup key will be emailed in a link to the customer.

Upon clicking the link, the customer will be directed to a user setup page. This user setup page will ask for a unique ID from the customer (not contained in the email or link), and this ID will be looked up in the database to make sure the setup key and ID are paired correctly. If the pair is valid, the customer will be asked to specify a username, password, and email address.

All security keys are currently 20-character alphanumeric strings. They are randomly generated and are set with an expiration date specified by Century Bank. They can be used up until the expiration date, but upon use, they are deleted from the database. For example, if the user forgets the username a second time in a week, he or she will need to go through the whole reset process again a second time—the first link will no longer work.

Next, the user will pick three distinct security questions and enter answers for each. Finally, the user will be asked to enter a personalized security greeting (to be shown on the password entry screen) and a security image.
Once these setup steps are complete, the user will be able to login for the first time.

General Login Process

On the main login screen, the customer will be asked to enter a username.

If the username entered is **valid**, the user is asked a random question from the list of three security questions. This same security question will be asked each time a login is attempted until it is answered correctly. If the user answers a certain number of times (set by Century Bank) incorrectly, the account is locked out. On this screen, the user has the option of having the PC remembered for a certain number of days (set by Century Bank), during which no security question will be asked again.

If the username entered is **invalid**, the user is asked a random question from the application’s full list of security questions. The security question may or may not be one associated with the user’s valid username. No matter what security answer is entered, the system will return an error of “Invalid answer for this user.” The system never indicates if just a username is invalid to protect against username enumeration vulnerabilities.

If the security question is answered correctly, the user is directed to the password entry screen. This screen displays the personalized greeting as well as the security image to assure the user that they are about to enter their password into the correct site and not an impostor. If the user answers a certain number of times (set by Century Bank) incorrectly, the account is locked out.
If the password is entered correctly, the user is logged in.

If password is forgotten

The user clicks "Forgot password" link from main login screen. The user is prompted to enter the username and answer a security question. If the security question is answered correctly, an email is sent to the address on file containing a link. The link contains a key which, when paired with the username, allows the user to enter a new password.

If username is forgotten

The user clicks the "Forgot username" link from main login screen. The user is prompted to enter the email address and answer a security question. If the security question is answered correctly, an email is sent to the address on file containing a link. The link contains a key that directs the main login page to prefill the username when the link is followed. The financial institution can optionally turn off the "Forgot username" links from showing up on their login screen.

Network Controls Between the end user and Internet Banking Host

SSL Protocol: All Internet Banking activity uses the Secure Sockets Layer (SSL) protocol. SSL is a set of formal rules describing how to transmit data to provide encrypted communications over the Internet. SSL protocol utilizes public-key cryptography to ensure privacy for the data moving between the browser and Internet Banking servers. This protocol allows for the transfer of digitally signed certificates for authentication procedures, and provides message integrity ensuring the data cannot be altered enroute. By convention, the URLs for the web pages that require an SSL connection start with https, instead of http.

Internet Banking websites have a certificate that is 2048 SHA-2 and only accepts TLS 1.0, 1.1 and 1.2.

Public-Key Cryptography: Public-key cryptography is used for encryption and server authentication. Encrypted messages provide protection against anyone eavesdropping; even if the information is intercepted, it is unreadable. Authentication identifies the origin of the information and that it has not been altered. Authentication also provides an extremely valuable tool in network security: verification of the identity of an individual. When an account holder wants to initiate a transaction, the browser is used to send a secure message via SSL to the web server. This method assures account holders they are actually communicating with web server, and not a third party who is attempting to intercept the transaction request.

Secure Network: All Internet Banking traffic must pass through a firewall, and filtering/screening routers. Traffic through the firewall is processed to a special proxy system, which operates similar to a filtering/screen router and verifies format, source and destination of each information packet. The proxy then changes the IP address of the packet and delivers it to the appropriate site. This protects inside addresses from outside access and makes the structure of the Internet Banking perimeter networks invisible to outside observers.

To understand the importance of this structure, think of Internet Banking as having a front door and a backdoor: the Firewall provides security at the front door and the Filtering/Screening Router provides security at the back door.