General Internet Resources

Determining Your Browser Version

Internet Explorer – click  > About Internet Explorer

Mozilla Firefox – click  >  > About Firefox

Google Chrome – click  > About Google Chrome

Safari – click Safari > About Safari

Other System Settings

The following settings and plug-ins are required to properly access online banking

- Cookies: Enabled (first and third party)
- JavaScript: Enabled
- Minimum Screen Resolution: 1024X768 pixels
- PDF Reader: Compatible*
- Adobe Flash Player: Latest version**

**Any compatible PDF viewer will suffice. For some operating systems and browsers (Google Chrome) PDF readers are built in with no need to install additional software. A common PDF reader is Adobe Acrobat Reader.*

***Adobe Flash is only needed for the FinanceWorks section of online banking*

What is Multifactor Authentication?

Your online security is important to us, as well as providing you easy and convenient banking tools. Your online banking experience may include a new Enhanced Login Security service to further help protect you from identity theft which is known in the online security industry as Multifactor Authentication, or MFA.

Authentication is the process used to allow access to only the correct person. Without effective authentication controls, it is possible for fraudulent users to access your account. We authenticate members by issuing challenges that only the true member should be able to pass.

Multifactor Authentication means that two or more different types (or factors) of authentication must be passed. By using two different factors of authentication, we get a higher assurance that the member is the intended user. MFA is commonly used to protect transactions at ATMs, where your card is something you have, and your PIN code is something you know.

For your convenience, after you successfully authenticate with your Username, password and Login Security (One-Time Passcode (OTP)), you may enroll your computer for use in authentication. If you choose to enroll your computer, a special Browser Cookie will be present on the system, which will act in place of your phone for something you have in your possession.

We recommend you ensure that your browser settings and any antivirus software you have do not delete your cookies (data files) so that you are not prompted to provide Login Security (One-Time Passcode (OTP)) every time you log into Online Banking. However, should you choose to delete your cookies (data files) you will be prompted to follow the multifactor authentication process.

Logging in from a computer you normally use?

When you choose to enroll your computer as PRIVATE, a special Browser Cookie will be present on the system, which will act in place of your Login Security (One-Time Passcode (OTP)). You will only need your Username and Password to access your account information.

If you are still getting prompted to provide your Login Security, then please review the following:

- There are no viruses or malware on your computer
- Your internet service provider isn't using a proxy server or web accelerator; for more information please contact them
- The settings for your browser follow our recommended browser settings
- Your browser is not set to delete cookies; please follow the browser settings for your respective browser in the recommended browser settings

Logging in from a computer you DO NOT normally use?

When you choose to list your computer as PUBLIC, you will need to provide your Username, Password and you will be prompted to provide your Login Security (One-Time Passcode (OTP)) each time you login to your account. We recommend this setting when logging in on a friend/relative's computer, at a library or when using other public computers.

Unable to Login to Online Banking

If you are using a recommended browser and are experiencing issues getting logged into online banking the issue may have to do with the internet provider. This is common with employer based internet access. Your employer may have firewalls, proxy servers or other equipment that may restrict access to secured sites; therefore we cannot troubleshoot or suggest changes to the computer settings.

Password

To ensure security we recommend the following: **NEVER REVEAL YOUR PASSWORD**

Password refers to your initial Call24 PIN number assigned when you first login to Online Banking and the password you select after your initial login. Passwords are case sensitive. If you have questions about what to enter in order to access Online Banking for the first time contact our Service Center at (800) 924-0022

Important

- Some browsers allow you to enable a function to require passwords for specific sites or certificates. In these instances you should enter the password for the browser NOT your online banking password
- Some browsers allow you to enable a function that will remember your password for the specific site you are logging into, we do not recommend utilizing this feature
- You can change your Online Banking password at any time under My Settings; you will be prompted to change your password every 180 days
- We do not have access to your password; in the case of a forgotten password please use the FORGOT PASSWORD link on the login page for Online Banking
- Always use Logout when you're done in Online Banking; do NOT use the back button - if you do not exit the Online Banking session the browser will allow you to use the back button to get back into your Online Banking session, this is NOT recommended

About Cookies

Cookies are small text files on your system, used to keep track of settings or data for a particular site. Websites can use cookies to identify a returning user or to pass information between webpages in a single visit.

There are two types of cookies: temporary and permanent. Temporary cookies are used and tracked by the browser to pass information and are deleted once the browser is shut down. Permanent cookies are stored on your system and can be accessed again for multiple visits. Permanent cookies usually have an expiration date and will be automatically deleted from your system at that time. Online Banking uses temporary cookies and may use permanent cookies, but never passes private information through cookies.

Online Banking also uses a different kind of temporary cookie known as a session cookie, a non-persistent cookie, or a pre-expired cookie. This cookie is used as part of the stringent security measures in Online Banking to make sure that each page in Online Banking is not cached or saved on your system. This means that each page must be retrieved from the webserver. This cookie is deleted when a user logs out or times out of Online Banking or if the browser window is closed and ensures that another user on the same computer cannot access the previous user's Online Banking session or information.

If you use Enhanced Security, Online Banking may place a secure permanent cookie on your computer. This secure cookie is unique, and when used in combination with your login information, creates a unique way to identify you to the system. For every login attempt after you add extra security to a computer, this secure cookie is validated along with the login identification you normally enter. This secure cookie is only used to validate your identity and does not contain any personal information.

About JavaScript

JavaScript is a widely accepted, simple programming language that allows a website to be more interactive. Websites can use JavaScript to perform many actions such as calculations, displaying dynamic navigation, and rotating through banner images. By using JavaScript, websites can be proactive by making a better internet experience.

An example of JavaScript in Online Banking is form validation. Validation is simply enforcing certain rules on different fields. When presented with a phone number field, JavaScript can alert the user if the phone number format is incorrect or if a value in the field is not a number. This allows the form to be filled out and submitted correctly the first time.

If JavaScript is not enabled, some or all of the Online Banking features may not work (ex. if you are asked to re-enter your password after you'd already entered your username and password). Please go to Java's website to confirm you've got the most recent version' after you've downloaded the most recent version confirm that Java is enabled in your browser by going to recommended browser settings.

In order to upgrade Java, please follow these steps:
-Go to www.java.com/en
-Click "Do I have Java?" link
-Click "Verify Java Version"
-Pop up will appear if Java needs to be updated. Have user click "Update"
-Click "Agree and Start Free Download" and click "Run" on the pop up that appears

About Secure Socket Layer (SSL)

Before initiating your Online Banking, we first require that a "secure session" is established using Secure Socket Layer (SSL) encryption. This is a process where the information between our Online Banking server and your browser is encrypted so it can't be read by unauthorized parties.

A general indicator that you have entered a secure session is when the URL (website address) in the address bar starts with a "https" (note the "**s**") rather than "http".

About Adobe Acrobat

Adobe Acrobat is a free browser plug-in that can read certain document file types known as PDF (portable document format). Having this plug-in allows you to read a PDF file from your browser window rather than having to open the Adobe Acrobat program to read the file. Most commonly PDFs are used in Online Banking to read eDocuments and images of checks. Please go to Adobe Acrobat's website to ensure you've got the most recent version for the best Online Banking experience.

Compatibility Mode

Microsoft's Internet Explorer has a feature called compatibility view that allows websites to better display older web pages. This mode is effective in taking old website that are not designed according to modern web standards and rendering them so that users can see and access them. Compatibility view can be triggered by a webpage that is not standard compliant or it can be enabled by a user.

Our Online Banking is designed according to the latest web standards and practices and to function without using compatibility view. If compatibility view is being used it can cause web pages that are standard compliant to display incorrectly. If compatibility view is enabled and a user is experiencing issues, the first step to troubleshoot is to disable this feature, as our Online Banking is compliant to web standards.