How We Protect You

Online Security

- Secure sign-on provides visual cues when you sign on so you know that you are on our website and it is safe to enter information.
- We have strict password standards. Password characters are masked as they are typed to maintain confidentiality. For internet banking clients, passwords must be at least six characters in length but no more than 10, are forced to be of multiple character types, cannot include more than three consecutive identical characters. User can change password as frequently as they feel necessary. We do not “force” a 90 day change but highly recommend the practice. Users should change password if they suspect it has been compromised. A password can not be reused in the past 15 cycles.
- We utilize secure socket layer (SSL) certificates to encrypt information.
- Account daily limits are set up for bill payment, funds transfer, wires, ACH and other treasury management services.
- We evaluate the latest security technologies and upgrade our systems whenever relevant improvements are available. We use advanced encryption technology such as intrusion detection and prevention systems, multiple firewalls, network and application access controls, multi-tier architecture and ongoing preemptive forensics to ensure your information stays safe and secure.
- We have implemented strict policies and procedures to safeguard your personal information to keep it confidential.
- We post Security Alerts to our website and alert users with scrolling message when new alerts are posted.
- We mask account numbers throughout the system.
- We provide cookies so that you do not have to enter answer security questions for each login.
- We require tokens for high risk transactions such as ACH and wire transfers.

Online Security FAQs

What is Secure Sign On?

Secure Sign On is a service to help protect you from fraudulent online activity. It provides you with visual cues when you sign on so you know that you are on our website and it is safe to enter information. Secure Sign On also helps us ensure that only authorized individuals can access financial information online.

How do I set up Secure Sign On?

By completing two easy steps. Set up confirmation questions that help us ensure that only authorized individuals are accessing your account information. Then, decide whether to register this personal computer as an authorized location from which to access your account information.

What happens if I cancel Secure Sign On during set up?

The information you enter in the setup process is not saved until you complete the final confirmation step and click “Submit.” If you exit the process before this final step, you will lose the information you have set up and will need to start the process again

Do I have to change any internet browser settings for Secure Sign On to work?

To register this computer as an authorized location for accessing your account information, your Internet Browser must be set to accept permanent cookies. Most browsers accept cookies as a default setting. If you haven't customized this setting, you'll probably not need to make any changes. If you do need to change the Internet cookie setting to accept permanent cookies, follow the instructions provided in the Internet browser's help file to complete this task. If you do not want to make this change, you will be able to sign on using the confirmation questions for validation.

What is *phishing*?

Phishing is an Internet fraud technique that is used by criminals to trick you into giving them personal information. Phishing occurs when a criminal sends you an e-mail message with a link to what may appear to be our website — but it is actually a fake. On this fake website, you will be asked to enter personal information, such as your social security number, account number or credit card number. Phishing is a fraudulent act aimed at stealing your identity and private account information. Phishers set up a phony website that looks like the site of a trusted company to trick you into disclosing your user ID and password.

How are the Secure Sign On confirmation questions used?

Confirmation questions are used as an additional form of identification when you sign on from a computer that has not been registered. They are also used to verify your identity if you forget your password or need to change a temporary password. These extra security measures help us insure that only authorized individuals access your financial information.

Can I change my confirmation questions?

To change your confirmation questions, log in to your account and go to the Options tab.

What happens when I register a personal computer?

We store a permanent cookie on the computer that enables us recognize it as an authorized location to access your information online. The next time you sign on, we will recognize the location and you will not be asked to answer confirmation questions as part of the sign on process.

What is a cookie?

A cookie is a small text file that a web server can store on a user's computer. The cookie we store on your computer is only used by us when you access your account information online. It is not used to track your Internet activity and cannot be used by others to access your information.

Why would I register a personal computer?

Registering your computer is another security measure to protect your financial information. With your user ID and password, this information helps us prevent unauthorized access to your accounts. On a registered computer, you are not asked to answer confirmation questions when you sign on — making it faster to access your account information.

Can I register my personal computer later?

Yes. Each time you sign on using an unregistered personal computer, you will be given an opportunity to register it.

Why shouldn't I register public computers?

We don't recommend registering public computers to access your financial information online. Public computers can be used by many individuals and aren't typically as secure as a personal computer. When you use public computers, we will ask you additional questions before you sign on to protect your personal information. Examples of public computers include, computers available at a library, coffee shop, or other public locations.

What happens if I register a personal computer by mistake? Can someone use it to access my account information?

No, someone cannot access your account information online simply because the computer has been registered. In addition to the cookie we use to register a computer, your user ID and password are needed to sign on from an authorized location. If you are concerned about a cookie that has been left on a public computer, we suggest that you change your password and/or user ID. The cookie does not contain this information and is useless if these other identifiers are not presented properly. Cookies are also updated periodically as an additional security measure.

If multiple people use this computer, should each person register it?

If more than one person is commonly using this computer to access information for accounts they have with us, each person should register the computer for faster access to their information. Registered locations are saved for each customer.

If I register this computer will I ever be asked to register it again?

You may be asked to register this computer again if the cookie is deleted or if your Internet browser doesn't allow permanent cookies. Also, if you use more than one Internet browser on your computer, you will be asked to register this computer the first time you use a different browser. Note: If your Internet browser doesn't allow permanent cookies, you can change your cookie settings using the instructions provided in the Internet browser's help file.

Are cookies dangerous to my computer?

No. Cookies are small text files that can only be retrieved by the website that stored it on your computer. These websites cannot look at any other cookie or anything else on your machine. The cookie we store on registered computers are only used to ensure that an authorized location is accessing your account information. It is not used to track your Internet activity and cannot be used by others to access your information.

Does anti-spyware and firewall software affect registration of a personal computer?

We recommend that you use anti-spyware and firewall software on all your computers. However, some anti-spyware and firewall software do not allow cookies to be stored on a computer. If your anti-spyware or firewall software do not allow cookies, you may not be able to register your personal computer. Some anti-spyware software may give you an option to remove cookies. If our cookie is removed, your personal computer will no longer be registered and you will be asked to answer confirmation questions the next time you sign on.

How can I guarantee the security of my banking and investment information?

You are the first line of defense for your online account security. We recommend that you:

- Never provide your user ID and password to anyone. Our employees never ask for this information.
- Be careful with your password. Do not write it down or maintain it in a place that is easily accessible.
- Select a password which consists of letters, a series of numbers, or a combination of letters and numbers that cannot be easily guessed by others.
- When you are done using Online Banking, exit the system by clicking the Sign Off or log out.

How do I access online banking if I forget my password?

Click the Forgot Your Password link on the Login page. If this link isn't displayed, please contact Customer Service for assistance.

How can I change my user id?

Following your initial enrollment into Online Banking, you will be permitted to change your user ID only once. While we do recommend that you change your password as often as needed to prevent it from being compromised, it is not wise to change the user ID, which uniquely identifies you as a user of the Online Banking service.