Security

Online Security

Enhanced Login Security significantly increases your level of protection online. Not only will your password and user ID be recognized, but your computer will be recognized as well. If we don't recognize your computer – you've logged in from a public computer or one you haven't used before - you will be prompted to provide information that only you will know. This step acts as an additional line of defense against unauthorized access to your accounts.

Safeguard your identity online.

In addition to protecting your email, there are a number of guidelines to follow that will help safeguard your identity online.

Do not allow a web site to keep sensitive information or credentials for future convenience.

It is a common practice when registering for access to a web site or making a purchase from a web site to be asked if you want to keep your access credentials, credit card number or other sensitive information on file as a matter of convenience. This common request is referred to as "remembering" for future use.

Be selective about where you surf.

Not all web sites are benign. Sites that are engaged in illegal or questionable activities often host damaging software and make users susceptible to aggressive computer attacks.

Don't choose "Remember My Password."

You should never use the "remember password" feature for online banking or transactional web sites.

Don't use public computers for sensitive operations.

Since you cannot validate the computer's integrity, there's a higher risk of fraud when you log in from a public computer.

Lock your computer when it is not in use.

This helps protect you from unauthorized user access.

Work on a computer you trust.

Firewalls, antivirus, anti-spyware and other protection devices help keep a computer properly monitored and provide peace of mind. These tools are important in order to protect your computer and data. A good firewall is critical if you commonly access the Internet via a wireless connection. It is also important to keep your computer up-to-date with patches to security tools as well as to the operating system and other programs on your computer. Make sure to configure your computer to update all security fixes.

Select a strong password.

The best password is an undetectable one. Never use birth dates, first names, pet names, addresses, phone numbers, or Social Security numbers. Use a combination of letters, numbers and symbols. Be sure to change your passwords regularly.

Use a secure browser.

Only use secure web pages when you're conducting transactions online (a web page is secure if there is a locked padlock in the lower left-hand corner of your browser).

Security

Online Security

Sign off, shut down, and disconnect.

Always sign off or logout from your online banking session or any other web site that you've logged into using a user ID and password. When a computer is not in use, it should be shut down or disconnected from the Internet.

Beware of shoulder surfing.

This is a common tactic that happens in public places such as coffee shops, airports, and libraries etc. where an attacker will look over your shoulder when you're logged in to obtain your sensitive information. Be vigilant and aware of prying eyes.

Set up a timeout.

The Timeout feature is an additional safety check. It can prevent others from continuing your online banking session if you left your PC unattended without logging out. You can set the Timeout period in the User Options screen.