Secure Web Browsing

All web browsers keep records of where you have been on the Internet and can potentially store web pages, data entered on web pages and site log-in credentials. Below are some good web security practices to follow:

- Whether the computer is shared with others or not, disable the web browsers ‘Auto-Fill’ or ‘Auto-Complete’ functionality to prevent log-in credentials and sensitive personal information you enter from getting stored in your web browser. Consult with the browser’s on-line help to determine how to disable this functionality.

- If the browser you are using supports multiple tabs and has saved this site as a ‘saved session’, delete the ‘saved session’. Consult with the browser’s on-line help to determine if browser is using tab browsing, ‘saved sessions’ and how to delete ‘saved sessions’.

- When you are done using the site, always click the site’s 'Log Out' link and perform the following browser clean-up on the computer before closing the browser for the web session you just had:
  - Delete all cookies
  - Delete cached web pages
  - Delete cached internet address history (and tabs)

- While using a Public Access Computer via an Internet cafe, airport Internet kiosk, or any other publically shared computer to access your personal data may be convenient, you must be aware of the potential risk involved. If you do not clear the browser's cache on the computer you use, someone else might be able to access your personal data. Or worse, the public access computer has been compromised with malware that steals your log-in credentials and personal information. We recommend to avoid using Public Access Computers altogether to access our site.

- Regardless of the location of the computer, always be wary of people that may look over your shoulder—they could potentially see your login ID, password, or personal data as you use this site.

- In regards to emails and instant messages containing website links, never click on the link. Rather copy the link out and paste into the address bar of the browser. Should an email or instant message come from a malicious source, this will avoid the possibility of being directed to a fake site, seeking to obtain account credentials or personal information or worse, trigger the download and installation of malware/spyware onto the computer.

- Be wary of any email or instant messages that instruct you to log into a secure site you use and then has you click on a link in the email/instant message. This is a technique cybercriminals use to execute actions of their choosing against targeted secure sites on your behalf. They do this by targeting and tricking you (the victim), into logging in the target secure site. The link they provided in their email/instant message contains the action the cybercriminal wants to execute. By you clicking on the link, the action executes. The cybercriminal’s link can appear harmless in the email/instant message, but once clicked the underlying action executes. The actions can range from making a purchase/transaction on your behalf, to changing your account credentials, too gaining real-time access to the secure site as you. If you receive an email/instant message instructing you do this type of activity,
contact the secure web sites customer support and have them confirm they send you the email and instructions. Contact your secure web site using the Customer Support information posted on the secure website itself, not what is contained in the email/instant message.

- When accessing internet websites, only use computers having up-to-date anti-virus and software firewalls or use some type of internet security software package (contains All anti-virus and firewall protection).

- How Secure is this? We recognize the sensitivity of the information that you are providing and protect it in several ways:
  - All internet communication between your browser and our system is sent using an encrypted channel (HTTPS) which is strictly enforced.
  - All personal information collected into our system is protected from unauthorized access and use utilizing security measures that comply with federal laws. These measures address the web site, computer safeguards, secured files and buildings.