Banterra constantly strives to make their customers aware of security threats and protecting your identity. **The recent "HeartBleed" threat has not affected Banterra's secure online, mobile banking and internal systems**, but we want our customers to be informed of the situation and steps they can take for additional protection for their personal needs.

Summary of Internet-Based Risk
"HeartBleed" is the name given to a critical vulnerability that has been identified within OpenSSL that was publicly announced on April 7th. OpenSSL is open-source encryption technology that is used by an estimated two-thirds of Web servers. Although the HeartBleed vulnerability was publicly announced on April 7th, the affected OpenSSL versions have been in use for more than two years.

Description
The vulnerability may allow unauthorized access to sensitive data including, but not limited to, passwords, usernames/IDs and private encryption keys. Many websites/systems use OpenSSL to encrypt data/communications within applications over the internet. An attacker/hacker could attempt to exploit this vulnerability by using malware (malicious software or application) to decrypt and/or acquire the sensitive data (passwords, usernames/IDs, private keys, etc.) or impersonate the site. Exploitation code (malware) is widely available and websites/systems that require a username and/or password to access the sites/system are most vulnerable.

What is the risk?
In simple terms, attackers/hackers could compromise usernames and passwords or decrypt any sensitive data in transit within the site/system over the internet (i.e. personal or account information).

What do you need to do?
1. We recommend that **IF** you use the combination of the same username and password for multiple sites, you should change your usernames and passwords to a unique username and password combination for each of those sites.

2. Contact the company/owner of the sites/systems you use that may contain personal or sensitive data to ensure there are no vulnerabilities with their site/system. If they have installed patches to the site/system to help protect it from the vulnerability, you should change your username and/or password used to gain access to those sites/systems after they have installed the patches.

Additional Information
For additional information regarding the "HeartBleed" threat, go to www.heartbleed.com.