Heartbleed?

You may have read in the media lately about the discovery of a wide-reaching Internet vulnerability called ñHeartbleed Bugò This serious security issue is the result of a flaw in the cryptography of popular OpenSSL software used to secure private information across the web, email, instant messaging and other Internet-connected routers and appliances.

The Heartbleed bug potentially allows hackers to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Most all affected systems are now properly patched for this bug and we believe that risks are limited to timeframes since the discovery on Monday, April 7th and the time systems were patched.

Mount Vernon Bank & Trust Company has been working diligently with our Internet Banking service provider since the OpenSSL issue was identified to assess and minimize any potential risk to our customers. As part of a comprehensive review and testing of our systems, it was determined that our IB (Internet Banking) was utilizing an OpenSSL version with the implementation flaw.

To address the immediate and underlying issues:

- On April 9, 2014, a patch was implemented by our provider to address the potential vulnerability. The implementation was tested and confirmed as valid.
- As a precautionary step, new certificates were issued. The new certificates were changed on Sunday, April 13, 2014.
- On the evening of Tuesday, April 8, 2014, our providerôs intrusion detection systems were updated to alert on attempts to exploit this specific vulnerability. Since that time, no alerts have been escalated. Prior to this, we have no evidence that the limited number of systems that would have been vulnerable had been improperly accessed due to this issue.

At this time, we are not requiring that you change your Internet Banking password, however if you accessed the system anytime from Monday, April 9th to Sunday, April 13, we would advise you to change your password at your earliest opportunity. As an abundance of caution, we would advise all of our Internet Banking customers to change their passwords from time-to-time to further protect unauthorized access. We strongly advise you to choose a complex password that is unique from any other Internet service or login that you use. Please contact any of our customer service representatives or bookkeepers if you require assistance.

We will keep you abreast of any further developments that may affect your security or usage of Mount Vernon Bankôs Internet Banking or any other services that we offer.

You should consider changing other passwords for other Internet services as the Heartbleed bug affected many popular websites and email providers. We again suggest that you use unique passwords for any website where you value the security and confidentiality of your private information.

Beware of phishing emails. Fraudsters are opportunistic and know that people may be worried about the recent Heartbleed flaw and could spam out a phishing attack disguised as a legitimate email from a web service asking users to reset their passwords.

Be suspicious of any unsolicited emails you receive, even if they are from companies you are familiar with, if they ask you to click on a link inside the email to reset your password rather than ask you to visit the website manually and login there instead.

For more information on the Heartbleed bug, you may visit these sites.

http://heartbleed.com/

https://lastpass.com/heartbleed/

http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/