PRIME MERIDIAN BANK™

April 11, 2014

SECURITY ALERT

HEARTBLEED BUG ALERT

Nicknamed "the Heartbleed Bug," a new online security flaw enables an attacker to steal secure content and the encryption keys protecting that content. It does this by tricking secure servers into spitting out chunks of data after rendering them vulnerable (no longer "encrypted").

When personal information is encrypted (ie: bank account numbers, passwords, etc.), encryption replaces the information you enter while it is being transmitted. This ensures hackers cannot read your sensitive information. For instance, encryption could translate a message as simple as "123456" to a "hashed" code like "F#h7er" before it reaches its recipient.

Secure servers are often used to store this personal information. But if the Heartbleed Bug is present, that information returns to being vulnerable again as the encryption gets stripped away.

Why is the Heartbleed Bug dangerous?

The Heartbleed Bug should be taken very seriously for the following reasons:

- the bug specifically affects "OpenSSL," a hub which stores encryption keys for two-thirds of sites on the web
- the bug also affects "OpenVPN"
- a large number of private keys and other secrets have been exposed to the Internet
- exploits leave no trace
- the bug has been unrecognized as a threat for approximately two years

How likely is it I am affected?

You are likely to be affected either directly or indirectly. Affected sites may include:

- Social media websites
- Business websites
- eCommerce websites
- Government websites

What precautions has Prime Meridian Bank taken?

At present, all of Prime Meridian Bank's vendors have reported back to us as not being vulnerable. Additionally, our servers and software have been verified as not being vulnerable.

What you should do.

>> CHANGE YOUR PASSWORDS

Some Internet companies vulnerable to the bug have already updated their servers with a security patch to fix the issue. This means you'll need to go in and change your passwords immediately for these sites.

However, ***even that is no guarantee your information was not already compromised.***

Although changing your password regularly is always good practice, if a site or service hasn't yet patched the problem, your information will still be vulnerable.

If you reuse the same password on multiple sites, and one of those sites was vulnerable, you'll need to change the password everywhere. *Note:* It is not a good idea to use the same password across multiple sites. (See our Password Tips).

Business owners: even if you change your passwords, you should work with your business partners to ensure vulnerable servers have had certificates reissued. (Otherwise you are not much more secure).

>> CHECK FOR VULNERABLE WEBSITES

The online resource link below can check websites and mail providers (e.g Google, Yahoo, Amazon) you may already be using:

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

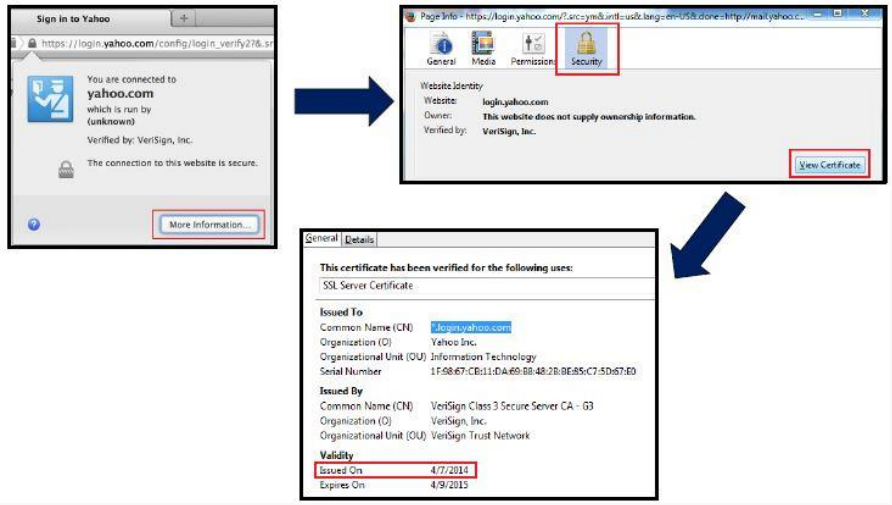
>> HEARTBLEED TEST SITE

Use the website below to check for vulnerable sites: http://filippo.io/Heartbleed/

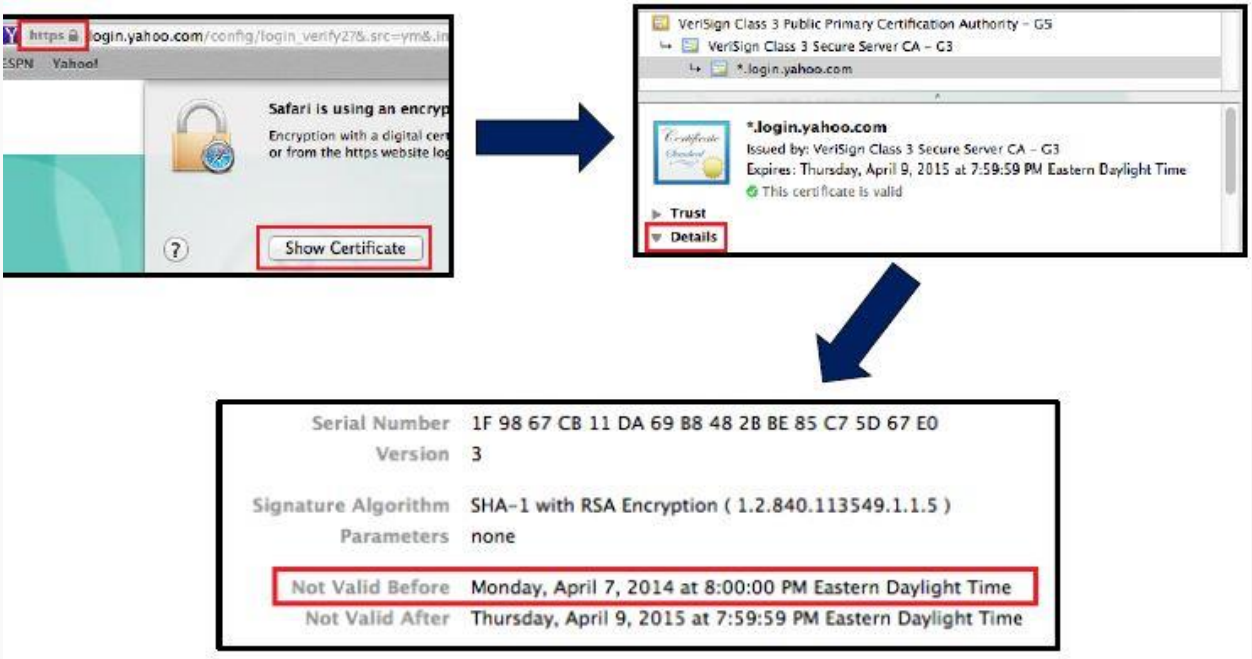
>> CHECK FOR OLD SSL CERTIFICATES

The small "lock" icon in your browser address bar generally lets you know you are entering information into a site with a secure Certificate. But, since the advent of Heartbleed, it is up to you to check for revoked or expired Certificates. Using the browser guide below, click on the lock icon to reveal details about Certificates you encounter. If the Certificate's Validity date is expired, the site is vulnerable.

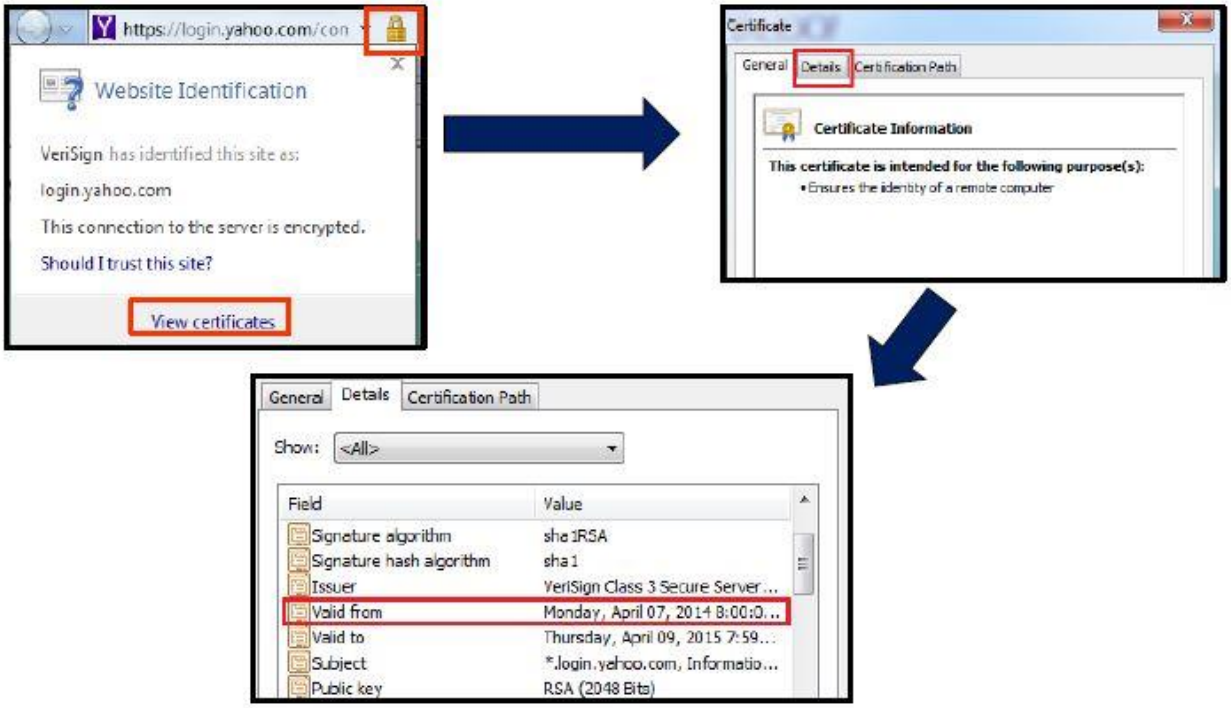
Firefox



Safari

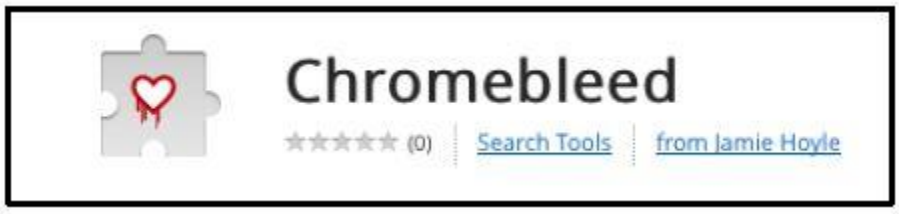


MSIE



Chrome

The ChromeBleed plugin shows whether the site you are communicating with is vulnerable.Click here for the plugin.



Still have questions?

If you have questions, please feel free to contact your Prime Meridian Bank representative directly or call 850-907-2300. Read more at HeartBleed.com.