Bug in HTTPS Protocol Means it is Time to Change Your Online Passwords

April 11, 2014 - This week it was discovered that supposedly secure websites that use the HTTPS protocol have a bug in them which would allow hackers to gain access to personal information. HTTPS is used by virtually every single website that requires users to log on with a password. And it includes sites like Google and Amazon. Here is what you need to know.

The bug is called Heartbleed. It was inserted into the HTTPS code about two years ago by mistake.

Since the discovery of Heartbleed, software providers have been rushing out code patches to companies that use HTTPS. Those patches will prevent hackers from exploiting the bug in the future. What isn't known however is if any enterprising hackers have been able to steal information already by using Heartbleed. If they have, the software patches won't be effective unless users actually change their passwords.

The internet users who are most vulnerable are those who use the same passwords on multiple websites. The reason for this is that if a hacker can steal your sign on information from a site that hasn't been patched, that information can then be used on another siteâ€¦ your online bank, for instanceâ€¦ even if it has been patched. Because of this, the only way that you can really protect yourself is to make sure that every site that you sign onto has a different password associated with it. While this may sound like an ominous task, there are a number of free password generators available that can do the job for you.

It is important to note that internet users are really at the mercy of the sites that they use to fix this problem. Even though

there are now Heartbleed patches available to website operators, it is up to those operators to install the patch on their systems. If they don't, then this vulnerability will continue to exist.

ACCESS is advising users to change their passwords now, and then again in two weeks. This will give website operators some time to make changes to their sites and will help protect users immediately.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS