



Cyber Alert: Heartbleed

What is Heartbleed

Heartbleed is a computer bug that attacks an organization's computer servers. A server has encryption software to protect passwords, user ID and other personally identifiable information. Heartbleed attacks that encryption software so that hackers could access this personal information, referred to as credentials.

How to Protect Yourself

There are steps you can take to help protect yourself at home. Many internet sites use encryption software to protect you as you conduct business with their company. As CNNMoney reports, "If you see a padlock image in the address bar, there's a good chance that site is using the encryption software that was impacted by the Heartbleed bug."

Most major websites rely on web server programs called Apache or Nginx to encrypt your information, and both have been vulnerable to Heartbleed. Organizations have been making fixes to their systems to prevent potential hackers from seeing un-encrypted information that Heartbleed may have caused. Amazon, Google, and Yahoo have all updated their websites to fix the problem, but others are still implementing "patches" to protect your information.

To help protect yourself, it is recommended that you log out of all websites on your personal devices including email, social media, and banking sites. This will give companies a chance to implement a new version of the encryption software to fix the bug. In the weeks ahead, you can change your password to try to protect yourself. A strong password has the following characteristics:

- Has at least eight characters
- Contains both upper and lower case letters (a-z, A-Z)
- Has digits and punctuation characters (0-9, !#\$%^&*()_+|~-=\`{ }[]: ";'<>?,./)
- Is not a word in any language, slang, dialect, or jargon
- Is not based on personal information (names of family, pets, co-workers, birthdays, etc.)