Overview
On Monday April 7th, a serious vulnerability was identified in one of the most popular implementations of the SSL protocol, called OpenSSL. SSL is a very important security protocol used throughout the Internet. Not only does SSL encrypt your online communications, but it helps ensure you are connecting to legitimate websites when you do things like shop or bank online. In this newsletter we give a very simple overview of what this vulnerability means to you and what you can do to protect yourself.

What Is Heartbleed?
The Heartbleed vulnerability allows a hacker to connect to a webserver and harvest sensitive information, which may include your login and password. If an attacker were able to harvest such information, they could use that information to log into any of your accounts using the same username and password. While the vulnerability has existed for the past two years, it was only discovered and publicly announced on April 7th. Heartbleed does not affect Windows or Mac computers; it primarily affects websites on the Internet that you use, such as Facebook and Gmail. To make matters more confusing, it does not affect every website on the Internet, but it does impact many of them. You can check if a website you use is or was vulnerable using the Lastpass site checking tool at https://lastpass.com/heartbleed/.

What Should I Do?
There are several steps you can take to protect yourself. Not only will these steps help protect you against the Heartbleed vulnerability, but they will help protect you against many other attacks in the future:

- First, change your passwords on websites that you know were vulnerable and have patched the vulnerability, starting with your most important accounts first. If you do not know if a website was vulnerable, go ahead and change your password anyway. This is a great time to update your passwords and improve your online security.
- Make sure when you update your passwords you use strong, hard-to-guess passwords. In addition, if the website supports something called two-step verification, enable it. This is an additional step that helps make your online account more secure. Finally, if your password has personal questions, we recommend changing the answers.
The best step to protecting yourself is to change your passwords on key accounts and make sure you use a unique, strong password for each one.

**Resources**

- Which Sites Are Vulnerable: [https://lastpass.com/heartbleed/](https://lastpass.com/heartbleed/)
- Technical Details: [https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105](https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105)

**License**

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 3.0 license](https://creativecommons.org/licenses/by-nc-nd/3.0/). You are free to share or distribute this newsletter as long as you do not sell or modify the newsletter. For past editions or translated versions, visit [www.securingthehuman.org/ouch](http://www.securingthehuman.org/ouch).

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

Securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus