

# [Heartbleed Bug](#)

Posted on Nov 25, Posted by [Paul](#) Category [Security and Scams](#)

The Heartbleed bug, a newly discovered security vulnerability that puts users' passwords at many popular Web sites at risk, has upended the Web since it was [disclosed earlier this year](#). It's an extremely serious issue, and as such, there's a lot of confusion about the bug and its implications as you use the Internet.

CNET has compiled a list of Frequently Asked Questions to help users learn more about the bug and [protect themselves](#). The Heartbleed situation is ongoing, and we'll update this FAQ as new issues arise. Check back for new information.

## **What is [Heartbleed](#)?**

[Heartbleed](#) is a security vulnerability in OpenSSL software that lets a hacker access the memory of data servers. According to Netcraft, an Internet research firm, 500,000 Web sites could be affected. That means a user's sensitive personal data -- including usernames, passwords, and credit card information -- is potentially at risk of being intercepted.

The vulnerability also means an attacker could steal a server's digital keys that are used to encrypt communications and get access to a company's secret internal documents.

[Heartbleed Bug: What you need to know](#)

## **How do I check if a website is vulnerable to Heartbleed:**

[LastPass](#)

[Qualys](#)

Please call for more information or if we can help you with anything else.

## **Computer Doctor**

Suite 1, Ground Floor Surfers Plaza Resort,  
70 Remembrance Drive,  
Surfers Paradise. Qld 4217

**Ph:** 07 55924733

**Fax:** 07 55924761

**Email:** [support@computerdoctor.com.au](mailto:support@computerdoctor.com.au)

**Web:** [www.computerdoctor.com.au](http://www.computerdoctor.com.au)

Tagged in: [malware](#) [security](#) [viruses](#) [webdesign](#)