

FAQ: Heartbleed Bug

What is the Heartbleed Bug?

Heartbleed is a flaw in the programming on secure websites that could put your personal information at risk, including passwords, credit card information and e-mails. The Heartbleed Bug is a defect in encryption technology – called Open SSL – used by most Web servers to secure users’ personal or financial information. It is behind many “https” sites that collect personal or financial information. Basically, it provides a secure connection when you are conducting a transaction or sending an e-mail online. Experts discovered the bug recently and warned that cybercriminals could exploit it to access visitors' personal data or to impersonate a website and collect even more information.

Am I affected?

Most active users of the Internet have likely been exposed, since a majority of websites – including Facebook, retail and even government sites – use the Open SSL software. But it is unknown whether any criminals have actually exploited the bug, and several major sites, like Amazon, have already installed patches. Most sites with an address beginning with “https” are vulnerable until the website operator fixes the bug and users change their passwords.

Is my bank account safe?

Yes, consumers are always protected from any unauthorized transactions. Let the bank know immediately if you suspect any unusual activity.

Banks are monitoring your accounts. They use many different systems to protect customers’ information including rigorous security standards, encryption, and fraud detection software.

What can I do?

As always, it is a good idea to update your bank password every few months. Also, monitor your account regularly and report suspicious transactions to the bank immediately. Beware of phishing scams – or e-mails with malicious links – that will attempt to get additional sensitive information from you.

What are banks doing?

Banks are researching the possible impact of the Heartbleed Bug and are taking appropriate actions to ensure that it has no impact on their customers. Most Internet banking applications are not impacted by this bug. Most financial institutions have a special layer of security that prevents this type of exploit and some don’t use Open SSL at all.