

Heartbleed Bug



The Heartbleed bug is a flaw in the OpenSSL method of data encryption used by many of the world's websites, which was actually put into the code accidentally two years ago. This means that many sites that you communicate with via an HTTPS connection may have been leaking your information to hackers.

When a computer makes contact with a web server, the web server and the computer keep checking that the connection is still live. This connection test is called a heartbeat. The heartbeat code in certain versions of OpenSSL had an error, that allows a hacker to extract decrypted information from the servers memory while the connection is live.

Many services have already been patched. You should change your password on these services now.

Gmail was affected but patched, change your password.

Yahoo was affected but patched, change your password.

Facebook unclear, change your password

Twitter was affected, but patched, change your password

Flickr was affected, but patched, change your password

Instagram was affected, but patched, change your password

Dropbox was affected, but patched, change your password

Tumblr was affected, but patched, change your password

Pinterest was affected, but patched, change your password

Netflix was affected, but patched, change your password

Wunderlist was affected but patched, change your password

OkCupid was affected, but patched, change your password

eHarmony unclear, but new certificate issued, change your password

American Funds, was affected, but patched, change your password

GoDaddy was affected, but patched, change your password

RackSpace was affected, but patched, change your password

Justhost was affected, but patched, change your password

Wordpress was affected, but patched, change you password

Question: If I don't do financial stuff with my computer, do I still need to change my password?

Answer: Yes, if you care about the safety of the people on your contact list, you will change your password to prevent hackers from using your identity to push out malware to the people that trust you.

Of course any other services where you have reused these passwords also need to be changed. You should have a unique password for every site that you subscribe to. You don't want a security breach on one account to expose all of your information.

BEWARE: Be on the lookout for scams arriving in your inbox requesting you to change your password that send you to fake sites. As always scammers are going to use fear against you.

The following cartoon from <http://xkcd.com/1354/> depicts the heartbleed memory leak.

HOW THE HEARTBLEED BUG WORKS:

