The Heartbleed Threat

How vulnerable are your accounts?

Provided by Ellen Dorle, CFP

A plague at the heart of the Internet. Anyone who ventures online should be aware of the risks posed by Heartbleed, the biggest threat to Internet security in at least a couple of years. All Internet users need to respond to its reality.

What is it? Heartbleed isn't a virus, but a software bug – a distressing flaw in web encryption technology, specifically a defect in the widely used Open SSL cryptographic software library.[1]

Heartbleed was recently detected by Google Security researcher Neel Mehta and researchers at Internet security firm Codenomicon. They determined that all versions of OpenSSL released between March 14, 2012 and April 7, 2014 contained the bug. This flaw in RAM is hugely problematic, as popular open-source Web servers like Apache and ngnix use OpenSSL to protect user security.[1,2]

What kind of damage can it do? SSL is the software that gives you the secure connection (https://) on assorted websites. Potentially, the Heartbleed flaw in OpenSSL can let identity thieves snare enormous numbers of username/password combinations from such websites – without a trace.[1,3]

What websites are still vulnerable? The list is changing (and fortunately, decreasing) daily. Head to the respected tech website Mashable.com for a frequently updated "Heartbleed Hit List" (Google "Heartbleed hit list" and you'll get there in a click).[4]

Some vulnerable websites have promptly patched the Heartbleed defect, and this means that you should be changing your password at those websites, which include Facebook, Pinterest, Google, Yahoo! and others. If you don't, you are leaving yourself open to identity theft.[4]

Fortunately, very few of the big banking and day trading websites use OpenSSL; none have reported security issues so far. LinkedIn, AOL, PayPal and eBay also report that they are unaffected. The IRS reports no problems with its website.[4]

How can you protect yourself? Head to Mashable.com's list to see where you must change your password. Change passwords at those websites, and don't use the same new password for one site at another.

Some people like to use password managers such as Dashlane and LastPass – these are software programs that generate random, unique and very strong passwords for websites you visit, and which automatically enter them for you. You will actually never know these passwords; they will be hidden behind a single master password.[5]

Italian cybersecurity specialist Filippo Valsorda has a tool (filippo.io/Heartbleed/) where you can test a website (specifically, its server) to see if it is suffering from Heartbleed. Type in the website address and hit "go"; if the website is "all good", it has been patched for Heartbleed, but your password should still be changed anyway as a precaution; if the test finds it "vulnerable," that means you should refrain from changing a password for the moment and wait for the site to be secured. If you change passwords prior to the site being secured, you may actually be putting yourself at greater risk than you previously were.[5,6]

Be safe, stay alert. While the response to Heartbleed has been necessarily swift, it reminds us that we need to be vigilant and that online security can sometimes be overstated. So change those relevant passwords for sites that have been patched, if you haven't done so already.

Ellen Dorle, CFP Dorle Financial, LLC 7957 Olentangy River Road Columbus, OH 43235
edorle@ellendorle.com www.ellendorle.com 614-880-0064 Fax: 614-880-0067

Citations.

1 - theatlantic.com/technology/archive/2014/04/the-5-things-to-do-about-the-new-heartbleed-bug/360395/ [4/9/14]
2 - tinyurl.com/pt4u4jd [4/8/14]
3 - forbes.com/sites/jameslyne/2014/04/08/heartbeat-heartbleed-bug-breaks-worldwide-internet-security-again-and-yahoo/ [4/8/14]
4 - mashable.com/2014/04/09/heartbleed-bug-websites-affected/ [4/12/14]
5 - slate.com/blogs/future_tense/2014/04/10/password_managers_can_protect_you_from_vulnerabilities_like_heartbleed.html [4/10/14]
6 - latimes.com/business/technology/la-fi-tn-heartbleed-test-check-safe-sites-20140409,0,2218732.story#axzz2ytqRwphB [4/9/14]