To: City of Albuquerque personnel
Date: 4/9/2104
Subject: New Heartbleed vulnerability affecting many secure websites

---

What is the Heartbleed Bug?

On Monday, a serious bug was discovered in the OpenSSL software that could exposes users' communications to eavesdropping in SSL encrypted websites. These websites could be any site that requires authentication such as a user name and password.

How many sites are affected?

There aren't precise statistics available, but the researchers who discovered the vulnerability note these vulnerable servers account for about two-thirds of the sites on the web.

What sites are affected?

It is impossible to determine if a site is vulnerable. Potentially any site requiring authentication using a password such as On-line banking, public email accounts etc. could potentially be affected.

The vulnerability: (CVE-2014-0160).

Test a website at: http://filippo.io/Heartbleed/ (this site tests for the vulnerability and will provide a yes or no if the site has been updated.

What can you do?

There's nothing users can do until the web services have made their sites secure. Wait a day or so. Then change the passwords on the web services you use.

Users will largely need to depend on individual sites to notify them about whether the flaw has been addressed. Many major web services, like Yahoo, have already released such notices.

Be patient: Immediately changing passwords could feed a new password into a website that has not yet fixed the flaw. Wait a few days to give the organization time to address this vulnerability.

Avoid using on-line transaction which require authentication for a few days. This would include on-line banking.