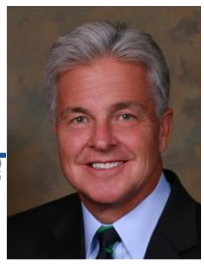
April 2014

For information about fraud and scams or to schedule a presentation about fraud related issues and prevention contact:

Maro Casparian
Dir. Consumer Fraud
amc@denverda.org
720.913.9036

DenverDA
Mitchell R. Morrissey, District Attorney - Second Judicial District
201 W. Colfax Avenue, Dept. 801, Denver, CO 80202
Bus. Phone: 720-913-9000
Fax: 720-913-9035



Mitch Morrissey
Denver District Attorney

Consumer Advisory

No Love Lost over Heartbleed Bug

Remember my consumer advisory back in February? I shared the best way to keep online information safe and secure is to make sure you are using a secure website. At that time I said a secure site will show a padlock icon and the address field will have "https" (the "s" means secure). Well, that was February and now, thanks to a computer bug called the Heartbleed bug, "S" may not be an indicator of security.

The Heartbleed bug has caused anxiety for people and businesses because it is affecting websites as well as networking equipment including routers, switches and firewalls. The extent of the damage caused by the Heartbleed bug is unknown. And unfortunately, there isn't much you can do to protect yourself completely until affected websites implement a security fix. This involves a two-step process by the website and then you will need to update your password for that website(s).

Most major sites, such as Google or Yahoo, will inform you when the fix has been implemented so that you can update your password.

Here are three things you can do to reduce the threat:

- First, determine if the websites you're surfing have been affected and/or updated. There are a number of sites that provide a way to check another site's vulnerability, such as Lastpass.com, Cnet.com and Mashable.com. These sites are continuously updating which websites are now secure so that you may then update your password(s) to be safe from the Heartbleed bug. Or go to the home page of your bank or website in question and see if they have provided any updates about the Heartbleed bug.

- Change your password(s). Once a website in question has put in place the required security patches, update your password(s) immediately.
  - When you change your passwords make them long and strong and make each password unique to each website. (Unless you have a better memory than mine, try LastPass, it's a terrific password manager)

- Check the website of the company that made your home router to see if it has announced any problems. Also be diligent about downloading and installing any software updates you may receive.

Denver DA's Fraud Line: 720-913-9179 ***Follow us on Twitter @DenverScamAlert***