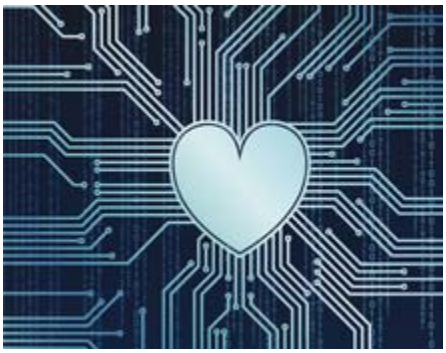
Avoiding ‘Heartbleed’

Security vulnerability did not affect postal websites



The “Heartbleed” bug hasn’t affected Postal Service websites that require customers to provide usernames and passwords, according to USPS IT and the Corporate Information Security Office (CISO).

“USPS was not vulnerable — nor is it today — to the threat that Heartbleed was responsible for creating,” said CISO Manager Chuck McGann. “Information Technology and Corporate Information Security continue to evaluate the situation on a daily basis and provide updates to our customers as warranted.”

Because the Postal Service was not using security software susceptible to the bug, its certificate keys are not susceptible to exposure, McGann said. However, USPS will update these certificates and work with Web service providers to monitor threats.

In addition, USPS has updated its websites to restrict access from older Web browsers. Employees and customers using browsers older than Internet Explorer 7.0 no longer will be able to access *usps.com*. Browsers now must support Advanced Encryption Standard, 256-bit encryption capability to conduct secure transactions with USPS websites.

McGann encouraged employees and customers who use the same login credentials for multiple websites to update their usernames and passwords on each site.

“The Postal Service is committed to providing a safe and secure online experience for customers,” said IT Manager of Marketing Relationship Management Robert Dixon. “We will continue to monitor the Heartbleed situation and protect sites accordingly.”