President's Corner: May, 2014
Batten Down the Hatches
By Eric Moore

Some software security issues have recently come up which you should be aware of. One is specific to Internet Explorer, while two others are threats to users of any number of different operating systems and web browsers. I recommend following up on these threats in order to protect yourself.

Internet Explorer Remote Code Execution Vulnerability
About a month ago, a flaw in Internet Explorer was announced to the public. This remote code execution vulnerability is named CVE-2014-1776. It could be exploited by an attacker to gain rights to your computer to cause Windows to perform any arbitrary operation, such as destroying data, controlling and shutting down Windows, installing malware, etc. The bug is rated critical for versions 6.0 through 11.0 of Internet Explorer. Security experts and the Department of Homeland Security advise users not to use Internet Explorer until the patch is installed. (Alternate web browsers such as Mozilla Firefox, Google Chrome, Apple Safari, and Opera are not affected.) Microsoft did soon after release a patch as part of Windows Updates. Kudos to Microsoft for releasing a patch for Windows XP, although Microsoft officially ceased to release security updates and patches for XP as of April 14, 2014. The easiest way to install the patch, kb2963983, is to run Windows Update and install any pending critical or recommended updates.

Source: https://technet.microsoft.com/en-US/library/security/2963983

Covert.Redirect
A bug was discovered about two weeks ago in open source software that is used by Facebook, Google, LinkedIn, and many other websites. The flaw called "Covert.Redirect" can be exploited to create a fake login pop-up window for a website and ask users to log in to use the app. Once the unsuspecting user logs in, the attacker can steal the user's login data and redirect them to a malicious site. There is no indication from Facebook that they will address the problem any time soon. The advice to users is if you click a link and are prompted to log into Facebook, close the pop-up.

Source: http://facecrooks.com/Internet-Safety-Privacy/Facebook-Other-Tech-Giants-Compromised-Open-Source-Bug.html/

Heartbleed Bug

At this month's CUGG meeting, I gave a short overview of a critical bug called "Heartbleed". (You will find a summary of my presentation with links for more information at http://www.cugg.org/docs/presentations/emoore/Heartbleed_Bug.pdf.) Heartbleed was discovered in early April and patched soon after. The bug—which has existed for more than two years—affects the OpenSSL software that is used by many—not all—websites that use SSL or TLS encryption. It could be exploited by an attacker to "read" sensitive data in the web server's memory. Such data could include passwords, customers' personal information, and security certificates used to decrypt incoming data from customers. Any site that you log into using a URL starting with "HTTPS" is *potentially* affected. Some of the resources linked to in my PDF list some sites that have been or are currently known to be affected. If a site that you use has fixed the problem, then you are advised to change your

password as a precaution. If any site you use is not listed, you are advised to contact the website's owner to learn if they are affected by Heartbleed and whether they advise you to change your password.

Sources:
http://heartbleed.com
http://en.wikipedia.org/wiki/Heartbleed
http://mashable.com/category/heartbleed/