



MEMORANDUM

Date: Tuesday April 15, 2014
To: EMS Services with SWORBHP Region
From: SWORBHP
Re: Heartbleed Bug - IMPORTANT NOTICE

SWORBHP has received notice from LHSC's ITS department that the www.sworbhp.ca server has been affected by the Heartbleed bug. The ITS department took immediate action to ensure our infrastructure was protected and secured. A patch has been applied and the server is no longer vulnerable to Heartbleed attacks.

Although we have no reason to believe that any part of our server has had unauthorized access, as a matter of best practice, we would recommend that all our users reset their passwords. To reset your password, visit www.sworbhp.ca (Paramedic Registry) and change your password in the Account Settings section.

Again, there is no reason to suspect that any unauthorized access has occurred.

The following information may help you better understand the Heartbleed bug issue. This bug allows attackers to send a small message to a web server, known as a Heartbeat and intended to let the server know they are still connected, and in turn bypass the SSL certificate (https) to obtain small amounts of unencrypted data stored in the server's memory. The big risk comes in the form of using this method to obtain usernames and passwords of users who have recently logged in to the vulnerable sites. Again, there seems to be no signs that this has happened for any of our accounts. This vulnerability has affected over half a million web sites, including Facebook, GMail, Yahoo Mail, and even the Canada Revenue Agency to name a few. The Heartbleed bug has actually existed for over 2 years, but due to the extremely complex nature in which it must be accessed, has only been discovered recently.

Regards,
SWORBHP