Office of the
Information &
Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency.

Information Bulletin

Apr. 11, 2014

Heartbleed: What you need to do to protect yourself

The Office of the Information and Privacy Commissioner has been following the Heartbleed exploit developments closely. We want to make sure that individuals and organizations are taking the necessary steps to protect personal information in the wake of this incident.

Heartbleed is not a virus – it’s a software flaw

What makes this exploit different from a virus is that this is a flaw in the software that sites use to secure passwords that you use to log in. It does not attack the user. Secondly, there is no forensic method to detect if the exploit was used or what personal information has been accessed (the exploit has been in place since the fall of 2011).

Change your passwords – more than once

While changing your passwords is a great practice and should be done in this instance, you may need to change them more than once. Most organizations have patched the exploit and are secure once again. Smaller websites (small business and personal) may not have patched their websites yet and therefore if you change all of your passwords and then use it on a site that is not yet patched, the new password is now jeopardized and may not be secure. Most security companies advise that you change your passwords now and change them again after a short period of time has passed to allow the smaller sites to patch their systems.

Another option is to change your password at sites after you verify that the exploit is patched. An online tool such as Last Pass verifies that the site is secure prior to you changing the password to a final version. In addition, many websites have compiled a list of top websites and whether or not they were affected by the Heartbleed exploit.

Check your website for vulnerability

Organizations need to check to see if their websites and computers are vulnerable to this exploit and patch them if this vulnerability exists. If you use SSL encryption on your website or computer hardware, it is especially important to check.

Organizations may also wish to prompt or force users to change their passwords if they were vulnerable to the Heartbleed exploit. In addition, if an organization confirms that they are vulnerable to the Heartbleed exploit, but the patch will take time to implement, they may wish to shut down their website until the vulnerability is fixed.

If your organization has been affected by Heartbleed and personal information may be involved, we encourage you to contact our Office for information and guidance on how to respond to the breach and take steps to remediate it. Call us at 250-387-5629 or email info@oipc.bc.ca if you have questions or want more information about how to respond to a privacy breach.