Heartbleed.ca: why cloud services and online banking sites should bolster security now

NEWS PROVIDED BY
Informatica Security Corporation ➞
Apr 11, 2014, 08:24 ET

TORONTO, April 11, 2014 /CNW/ - From the first reports of the Heartbleed OpenSSL bug earlier this week, IT departments have scrambled to reduce their exposure to the risk and notify concerned users about the safety of their personal information. But access to sensitive websites still needs to be more secure, according to Canadian security experts:

- once servers are patched and verifiably secure, companies should **not** rely on users to reset their own passwords: **passwords should be reset by the company**
- **cloud-based services** must responsibly notify their users of **all the impacted 3rd party sites** that may have played a part in the user experience, not just their own
- **online banking systems** should take the opportunity to introduce better security using **two-factor authentication**, ensuring that access doesn't just depend on user passwords

"*It's time Canadian banks offered the added security of a one-time code or token to better protect all their online customers*" said Claudiu Popa, security auditor and author of two books on data protection. "*It should be available on all sites that handle sensitive personal information, not just those that have been impacted by this latest issue*".

Multi-factor authentication vastly reduces breach impact with the need for another code that can only be used for a single visit so stolen passwords cannot be reused in the future.

Many global banks, along with sites like **Google, Facebook, Twitter, Yahoo, Dropbox, Paypal, Microsoft, iTunes and LinkedIn** offer optional two-factor authentication.

Canadian companies should take the opportunity to **gain a competitive advantage** with multi-factor authentication (MFA) and perfect forward secrecy (PFS), technologies that have been available for a long time.

About the company:

Established in 1989, Informatica is Canada's first security assurance-as-a-service company, specializing in standards-based IT audits, independent privacy and vulnerability assessments across all industry sectors.

Informatica's respected Statement of Trust™ and Verify™ seal are available to organizations that test their security with privacy audits and standardized risk assessments. Reviews of policies, employee awareness and website availability/stress-testing demonstrate compliance, leadership and due care.

Pre-audits for PIPEDA, CASL, PCI-DSS(3.0), ISO 31000/27000, PHIPA, Bill198, etc are conducted by certified security professionals and trusted Risk Advisors.

SOURCE: Informatica Security Corporation

For further information: Claudiu Popa, CEO, Informatica Corporation, email: Soundbites@SecurityandPrivacy.ca, www.SecurityAssessments.ca, Twitter:@datarisk, 1 Yonge St. Toronto, Canada, 416-431-9012