Canadian Mental Health Association,
Kamloops Branch
651 Victoria Street
Kamloops BC V2C 2B3

NOTICE OF INTERNAL SERVER BREACH

On Tuesday Sept. 8th, 2020 at approx. 7:30pm we became aware of a server related security incident pertaining to stored documents/information on the CMHA Kamloops server. The initial complaint was that file names were appearing that did not seem to make sense (e.g. BobGreen85@criptext.com). Upon our investigation we determined that the server had been compromised and the hacker had deleted a number of files. In addition, other files were made inaccessible through an encryption process.

Shortly after we discovered the hack, a screen message appeared from the hacker confirming the cyber-attack with instructions on how to re-obtain access to the data by making a ransomware payment in bitcoins.

Our understanding is that the machine, which may have allowed the hacker access to the server was turned off to avoid potentially exposing any other data. However, by this time, the server was being remotely controlled by the attacker. Steps were taken to restrict the hacker from being able to leverage their access to other systems, or users' machines.

It is not clear that any data was remotely accessed or downloaded to the attacker's computer. In our experience, ransomware attacks are generally about making information inaccessible so it can be held until a ransom to release it is paid. Attackers generally, do not copy or download data and would require a great deal of time and effort to do so. However, any data breach is significant and must be viewed with the potential that information may have been exposed.

Efforts were undertaken to wipe the server remotely and clean the server so that it could be reloaded with a new operating system. The data was restored via a combination of backups and decryption techniques. All users have been added back to the server and were scrutinized for legitimacy. Passwords were changed.

Our investigation found that the server data was compromised through a hacker using an administrator account. The most likely path for the attacker was by gaining access to a vulnerable user's workstation.

With the system restoral, an overall hardening of security measures has been undertaken and includes a recommendation to an overall review of internal privacy and data security policies. Some of the measures include the following:

- Currently, all users' machines connecting to the server are now mandated to have a robust antivirus enabled, in addition to being required to use a supported operating system like Windows 10 to ensure secure access.
- Brute force attack prevention software has been installed on the server.
- A process has been started to have users connect to the server via VPN.

Canadian Mental Health Association,
Kamloops Branch
651 Victoria Street
Kamloops BC V2C 2B3

- Policy of least privileges has been adopted.
- The user access lockout policy has been modified.
- The backup strategy for local and offsite has been modified to reduce the likelihood of a hacker gaining access.
- Server notifications have been enabled to report alerts such as high CPU usage.
- Email attack awareness documents have been made available to staff.

Additional security measures which will be explored and discussed for future implementation include the following:

- Intrusion detection software.
- Vulnerability scanning.
- Security awareness education.

How will this affect me?

Information and records from our donors, community partners and funders are stored outside of the server and protected using high-level encryption to protect your data. The remote server was **ONLY** for day-to-day operational use and collection of data within our programs.

Your next steps:

If your information was compromised for example your name and date of birth, it may put you at the risk for identity theft. Identity theft is when someone steals your personal information to open new accounts or commit activity using your name.

We encourage you to monitor your credit and remain vigilant in checking your financial statements.

1. Monitor your credit score

After incidents like this, it's important to monitor your credit score and be aware of any changes. If you don't know your credit score, you can check yours for free here. Pay close attention and monitor for suspicious activity.

Call Canada's main credit reporting agencies and put a fraud alert on your credit report:

1. Trans Union Canada (1-866-525-0262, Québec 1-877-713-3393)
2. Equifax Canada (1-866-779-6440)

2. Monitor your credit card statements and bank accounts

Canadian Mental Health Association,
Kamloops Branch
651 Victoria Street
Kamloops BC V2C 2B3

It is important to monitor it. Keep an eye out for any transactions you did not authorize and report any issues to your bank or credit card company right away.

3. Report any theft or crime

If you identify a concern that involves a theft or crime, report the incident to the local police. You should also report scam or fraud to the Canadian Anti-Fraud Centre. Tell your bank and credit card companies and close any accounts and cards that may have been compromised immediately.

For more information, please contact kamloops@cmha.bc.ca