Yukon Information and Privacy Commissioner

211 Hawkins Street, Suite 201
Whitehorse, Yukon Y1A 1X3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.ombudsman.yk.ca

Advisory regarding Zoom cyber security incident

Issued April 16, 2020

The Yukon Information and Privacy Commissioner (IPC) is issuing this advisory to inform Yukoners about a recent cyber security incident involving the Zoom videoconferencing application.

The IPC is aware that a number of organizations, businesses and individuals in Yukon are using Zoom to communicate while working remotely or to socialize online. A number of news outlets are now reporting that Zoom suffered a cyber security incident that may put the personal information of its users, and potentially that of others, at risk.

This incident creates risks that the IPC wants Yukoners to be aware of, so that they can take steps to protect themselves. The information provided in this advisory is intended to help Yukoners reduce these risks.

Nature of the incident

Numerous news outlets are reporting that Zoom suffered what is called a credential stuffing attack. In this type of attack, stolen account credentials, typically consisting of lists of usernames and/or email addresses and the corresponding passwords (often from a previous data breach) or slight variations of these passwords, are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application. Cyber criminals use specially-written computer code to automate the login process to the service using these credentials, such as those obtained via the 2016 LinkedIn breach.[1]

Reports indicate that personal information such as Zoom usernames, passwords and other details are currently for sale on the dark web.[2]

[1] https://fortune.com/2016/05/18/linkedin-data-breach-email-password/
[2] https://en.wikipedia.org/wiki/Dark_web - See section on dark net markets.

Security firms[3] confirm that the appearance of these credentials and Zoom host-keys[4] on the dark web have all the telltale signs of a credential stuffing attack. Just as recently happened with Disney Plus,[5] when a new service is launched, or an existing service gains in popularity, it is scrutinized by cyber criminals for weaknesses that can be used to turn a profit. Larger organizations, such as Google and Microsoft, often deploy technology that defends against this kind of attack. However, some organizations do not use this technology.

Zoom has responded to the incident with the following statement[6]:

> *"It is common for web services that serve consumers to be targeted by this type of activity, which typically involves bad actors testing large numbers of already compromised credentials from other platforms to see if users have reused them elsewhere. This kind of attack generally does not affect our large enterprise customers that use their own single sign-on systems. We have already hired multiple intelligence firms to find these password dumps and the tools used to create them, as well as a firm that has shut down thousands of websites attempting to trick users into downloading malware or giving up their credentials. We continue to investigate, are locking accounts we have found to be compromised, asking users to change their passwords to something more secure, and are looking at implementing additional technology solutions to bolster our efforts."*

It should be noted, that enterprise single sign-on itself does little to guard against credential stuffing attacks. Additional security is only provided when appropriate account lock-out settings and multi-factor authentication is configured.

What to do

As a result of this incident, any Yukoner who has activated a Zoom account is advised to reset their Zoom account passwords, taking care not to re-use old passwords, common passwords or slight variations of either.

For organizations with employees, proper end-user training on account and password management should be given, at least annually, to all employees to enable them to distinguish between good and bad practices.

If employees used their corporate email address to sign up for a Zoom account, and have re-used their corporate password, their work account passwords should be reset and the account should be monitored for indicators of compromise.

[3] https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/
[4] https://support.zoom.us/hc/en-us/articles/205172555-Using-your-host-key
[5] https://www.wired.com/story/disney-plus-hacks-credential-stuffing/
[6] https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/

If any Zoom accounts have been compromised, organizations need to evaluate if a breach of personal information or personal health information has occurred. Zoom has the ability to store chats, and transfer documents via the chat. Depending on Zoom settings, chats may be stored (automatically) for future access. If accounts have been accessed, and documents or chats contain personal information or personal health information, a breach will have occurred, unless it can be proven that the information was not accessed.

Organizations should evaluate their use of Zoom, as recently there have been multiple security and privacy incidents, as well as reports on vulnerabilities.

If organizations continue their use of Zoom, it is strongly recommended that they evaluate settings and practices according to the guidance issued on April 8, 2020, by the Yukon IPC on the use of video-conferencing and chat applications and the guidance provided by the Canadian Centre for Cyber Security on the use of video-teleconference software.[7]

Breach reporting requirements

Certain public bodies that are subject to the *Access to Information and Protection of Privacy Act* (ATIPP Act) have an obligation to report breaches of personal information according to the Yukon government corporate breach policy.

Custodians subject to the *Health Information Privacy and Management Act* (HIPMA) have an obligation to report breaches of personal health information, if there is a risk of significant harm to an individual as a result of the breach.

Private sector businesses that are engaged in commercial activity have a duty to report breaches of personal information in certain circumstances to the Privacy Commissioner of Canada under the *Personal Information Protection and Electronic Documents Act.*

The purpose of this document is to inform Yukoners about the risks to privacy associated with a recent cyber security incident and to support public bodies subject to the ATIPP Act and custodians subject to HIPMA in meeting their privacy and security obligations under these laws.

This document is not intended as, nor is it a substitute for, legal advice. This document is not binding on Yukon's Information and Privacy Commissioner.

[7] https://cyber.gc.ca/en/alerts/considerations-when-using-video-teleconference-products-and-services