Sitka

Sitka Follow-up on Co-op's April 19, 2024, Cyber-Security Incident

BC Libraries Cooperative sent out a Co-op wide notice on Wednesday April 24, 2024, about a security incident we experienced on April 19, 2024. We are now following up with members using specific Co-op services, as the incident had implications for your patrons' information.

The leaked log file contained the email address of anyone who received an email and the phone number of anyone who received an SMS message from a Co-op service between March 27 to April 19, 2024. This includes Sitka patrons who received automated notifications by email or SMS message for things like checkout receipts, overdue notices, and holds notifications during that period.

Only the email addresses of people who received notifications or the phone number of people who received SMS notifications were leaked. The content of the notifications was NOT leaked. The leaked data does not say what the notifications were about, and it does NOT reveal any other information about patrons or their library use, such as checkouts and holds.

The exploit which allowed the attacker to gain access to this log file was closed on April 19, 2024.

What to Do Next

Each Sitka member institution will be governed by specific privacy legislation. For public libraries, post-secondary institutions, government organizations and K-12 schools in BC, that is BC FOIPPA's legislation. Manitoba and Ontario libraries have their own privacy policies that govern them. Special libraries may fall under different legislation.

Regardless, the steps to take once you have received a notification of such a breach are generally similar across legislation - understand the seriousness of the harm of the breach, based on this decide if you are required to notify users and the privacy office that governs your specific organization.

Member libraries ultimately need to make their own assessment of harm. *To the best of our understanding, the leaked data is limited to email addresses or phone numbers of people who received automated notifications at a specific time; no other identifying information, no contents or subject lines of emails, nor any information about people's checkouts, holds or fines were leaked*. The Co-op believes the main harm that can come from the leaking of this information is a potential increase in spam, phishing or spear phishing attacks.

If you deem this a serious enough risk of harm that affected patrons need to be notified, then you need to follow the guidelines of the privacy legislation that governs your specific organization. For example, in BC public bodies governed by FOIPPA need to follow these guidelines https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/guidance-on-mandatory-privacy-breach-notifications and in Manitoba, public bodies governed by FIPPA need to follow these guidelines: https://www.ombudsman.mb.ca/info/privacy-breaches.html. Please ensure you follow the guidelines of the privacy legislation that governs your organization.

Notifying Patrons of Breach

We are unfortunately not able to provide a comprehensive list of your specific patrons that may have been affected. Thus, libraries likely must choose what is described as "Indirect notifications"; this may be a post on your website and a banner on your public catalogue or discovery layer.

You are ultimately responsible for your patrons' privacy and for communicating with them. We have provided some sample text that libraries may use below.

Sample Notices

Co-op staff have provided sample text (in Word format) to customize and add to your website, as well as suggested text to post on a banner on the public catalogue. Please contact Co-op Support at sitka@bc.libraries.coop if you wish to add a banner to your Evergreen public catalogue.

Notifying the Privacy Commissioner

In addition, most privacy legislation will also include a requirement for the public body to disclose the breach to the governing privacy body. Such a disclosure might take the form of an email to the privacy commissioner or ombudsman such as:

"Notification to Privacy Office of Privacy Breach

On April 25, 2024, our ILS (integrated library system) provider, the BC Libraries Cooperative, (the Co-op) notified us that they had experienced a security incident. Log files on their servers were obtained that contained the email addresses and phone numbers of patrons who had received automated notifications from the library system (i.e., checkout notices, overdue notices, hold notifications) between March 27 and April 19. This is the limit of what was obtained – patron email addresses and phone numbers and nothing else. The Co-op informed us that the exploit which allowed the attacker to gain access to this log file was closed on April 19, 2024, the Co-op is not able to provide a specific list of affected emails, therefore we are required to take an Indirect Method of contact with our patrons. We have placed a notice on our website and have also linked to that notice from within the affected software, describing the extent of the breach and steps patrons can take to help combat any resulting spam or phishing attempts."

Still have questions or concerns?

Please feel free to contact Scott Leslie, Systems Manager, Privacy and Security Officer, BC Libraries Cooperative Tel: (250) 415-3490 Email: scott.leslie@bc.libraries.coop