What to do in case of suspected data breach

In the case of suspected data breaches ie a committee members phone is stolen, or there is a break in and your laptop (which is left logged in) is stolen, please follow the below steps to help secure your data and email admin@setls.com.au

LOG OUT THE USER (pictured)

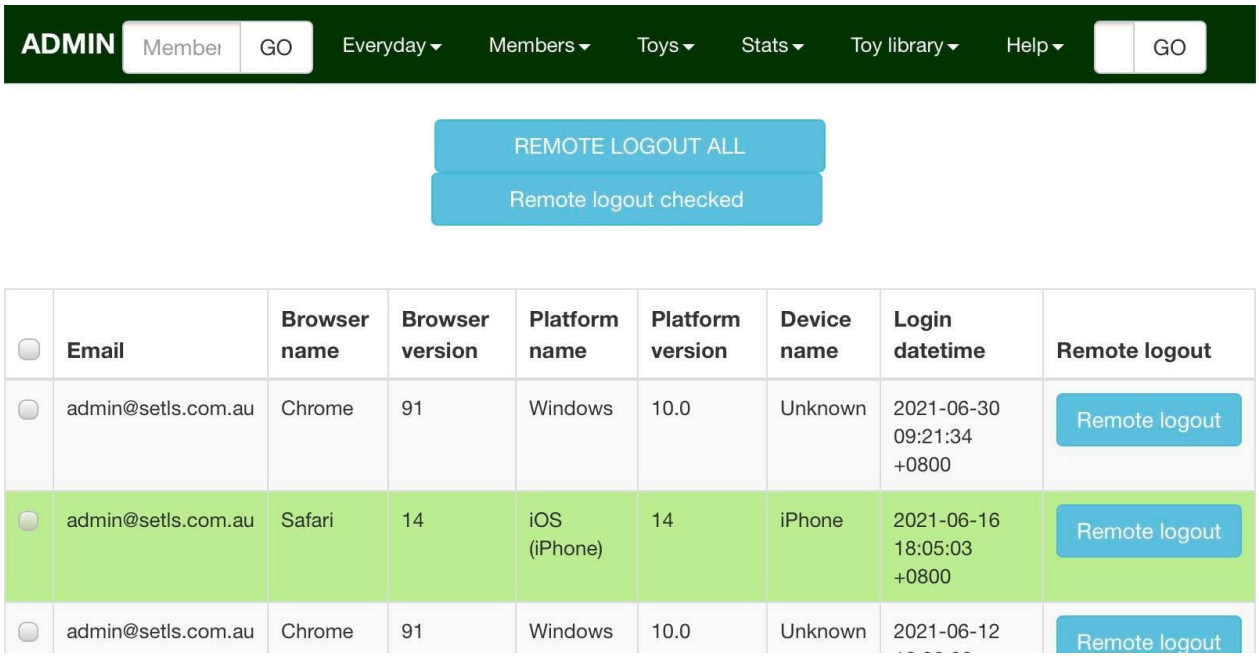
If you are confident in which user/s are logged in/saved on the devices, go to their account and select login history. You have the option of logging out specific sessions, or logging all sessions out. If it is your own account that has been compromised, logging all out will boot you out, so you may want to have another committee member on standby to do the next steps.

REMOVE ADMIN PRIVILEGES

Go to Profile, edit, and change Security Level to normal. This means that even if the person manages to log in, they won't be able to access anything other than that account's details.

RESET PASSWORD
Go to Username/Password, and generate a new password. This means that the password saved on the device will no longer work.

Note: I know some toy libraries also leave their emails logged in on their laptops, so there is a chance that if you email out the new password it will be received by the thief, which is why its so important to revoke those admin privileges.



Revision #2
Created 1 January 2022 06:32:01 by Caris Morris
Updated 16 August 2022 11:33:28 by Caris Morris