VMC Cloud Audit for July-September 2019

October 17th, 2019

Overview & Executive Summary

I performed a cloud audit for several of the Visit Mendocino County's cloud based information systems, looking at the security settings for each account as well as looking through the audit logs for suspicious or unusual activity. I audited the following systems: Dropbox, GSuite, and LastPass.

Issues Discovered

No major problems were discovered, but a few things require additional attention:

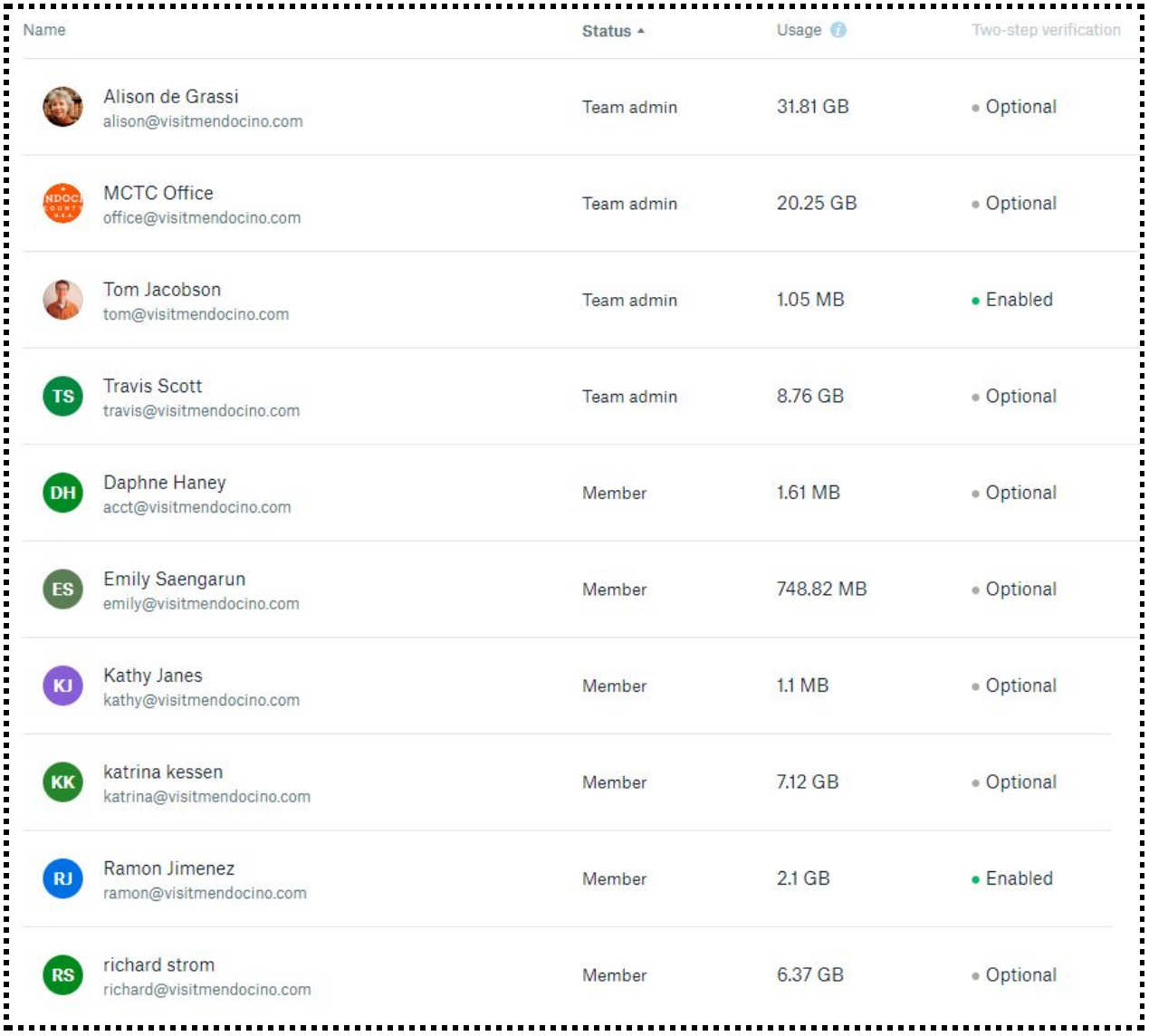
1. **Dropbox**: **RICHARD STROM, WHO IS NO LONGER AN EMPLOYEE OF VISIT MENDOCINO COUNTY, STILL HAS AN ACTIVE DROPBOX ACCOUNT - THIS SHOULD BE SUSPENDED AND HIS SYNCED DATA SHOULD BE DELETED. THERE IS NO EVIDENCE FROM THE DROPBOX AUDIT LOGS THAT RICHARD HAS TRIED TO ACCESS ANY DATA FROM DROPBOX SINCE HE LEFT THE ORGANIZATION.**
2. **Dropbox**: **ONLY TWO (2) OF THE TEN (10) DROPBOX FOR BUSINESS USERS HAVE TWO FACTOR AUTHENTICATION (2FA) TURNED ON FOR THEIR ACCOUNTS. VMC SHOULD TRY TO GET 100% OF USERS TO ENABLE 2FA.**
3. **Dropbox:** **DONNA HANNAFORD IS STILL HAS A DROPBOX FOR BUSINESS ACCOUNT, EVEN THOUGH IT IS DISCONNECTED. VMC IS NOT PAYING FOR THIS LICENSE, BUT IT SHOULD BE DELETED IF IT IS NOT NEEDED.**
4. **Dropbox:** **ENCOURAGE ALL VMC EMPLOYEES TO PERFORM THE DROPBOX SECURITY CHECKUP. THIS MUST BE DONE INDIVIDUALLY FOR EACH ACCOUNT.**

5. **Google:** ONLY THREE USERS, TRAVIS, RAMON, AND TOM, ARE USING TWO-STEP VERIFICATION FOR GSUITE. VMC SHOULD THINK ABOUT REQUIRING THIS BY POLICY LIKE IT DOES FOR LASTPASS.
6. **Google:** DUE TO THE WAY IN WHICH JENNIFER SEWARD'S GSUITE ACCOUNT WAS CREATED, A FULL ACCOUNT REVIEW OF HER ACCOUNT SHOULD BE PERFORMED TO MAKE SURE NONE OF JOHN KUHRY'S PERSONAL INFORMATION IS STILL CONTAINED IN HER ACCOUNT.
7. **LastPass**: abc. KATHY IS NOT USING LASTPASS AT ALL TO ACCESS THE ORGANIZATION'S ACCOUNTS.

Dropbox Audit

Review of Active Accounts and 2FA

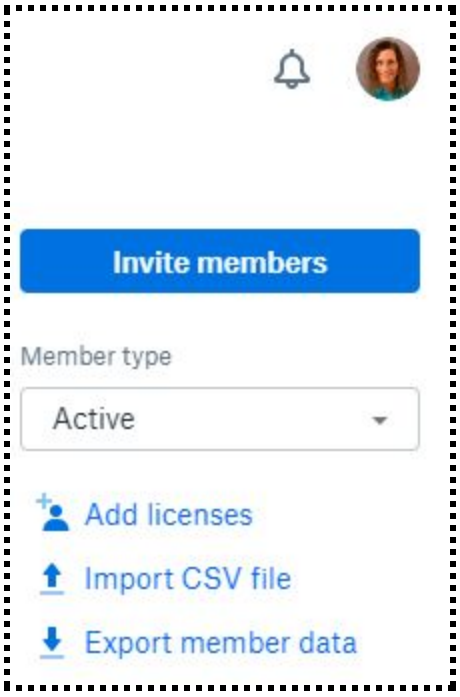
There are no unexpected member accounts in Visit Mendocino County's Dropbox for Business account. Only two out of ten members have two-step verification enabled. As of 10/4/19 only Tom Jacobson and Ramon Jimenez had two-step verification turned on. See image below, where Two-Step Verification is listed as Optional. Richard Strom, who is no longer an employee of Visit Mendocino County, still has an active Dropbox account - this should be suspended and his synced data should be deleted.



Name	Status	Usage	Two-step verification
Alison de Grassi alison@visitmendocino.com	Team admin	31.81 GB	Optional
MCTC Office office@visitmendocino.com	Team admin	20.25 GB	Optional
Tom Jacobson tom@visitmendocino.com	Team admin	1.05 MB	Enabled
TS Travis Scott travis@visitmendocino.com	Team admin	8.76 GB	Optional
DH Daphne Haney acct@visitmendocino.com	Member	1.61 MB	Optional
ES Emily Saengarun emily@visitmendocino.com	Member	748.82 MB	Optional
KJ Kathy Janes kathy@visitmendocino.com	Member	1.1 MB	Optional
KK katrina kessen katrina@visitmendocino.com	Member	7.12 GB	Optional
RJ Ramon Jimenez ramon@visitmendocino.com	Member	2.1 GB	Enabled
RS richard strom richard@visitmendocino.com	Member	6.37 GB	Optional

Export Dropbox Member Data

From the Members tab, choose Export member data link. This will create a report in a folder in VMC's Dropbox. Travis will receive an email once the report is ready.



Member Data Report 10/04/19

First name	Last name	Role	Status	Usage (in MB)	2FA
Alison	de Grassi	Team admin	Active	32,578.42	Optional
MCTC	Office	Team admin	Active	20,730.99	Optional
Tom	Jacobson	Team admin	Active	1.05	Enabled
Travis	Scott	Team admin	Active	8,970.61	Optional
Daphne	Haney	Member	Active	1.61	Optional
Emily	Saengarun	Member	Active	748.82	Optional

Kathy	Janes	Member	Active	1.1	Optional
katrina	kessen	Member	Active	7,288.29	Optional
Ramon	Jimenez	Member	Active	2,152.64	Enabled
richard	strom	Member	Active	6,521.39	Optional
Donna	Hannaford	Limited admin	Disconnected		Optional

Run Dropbox's Security Checkup

Run the Security Checkup (https://www.dropbox.com/account/security then Start Checkup). *Note that this is only for individual accounts; it does not cover the organization as a whole*. Encourage everyone at VMC to perform this security checkup, which covers the following areas:

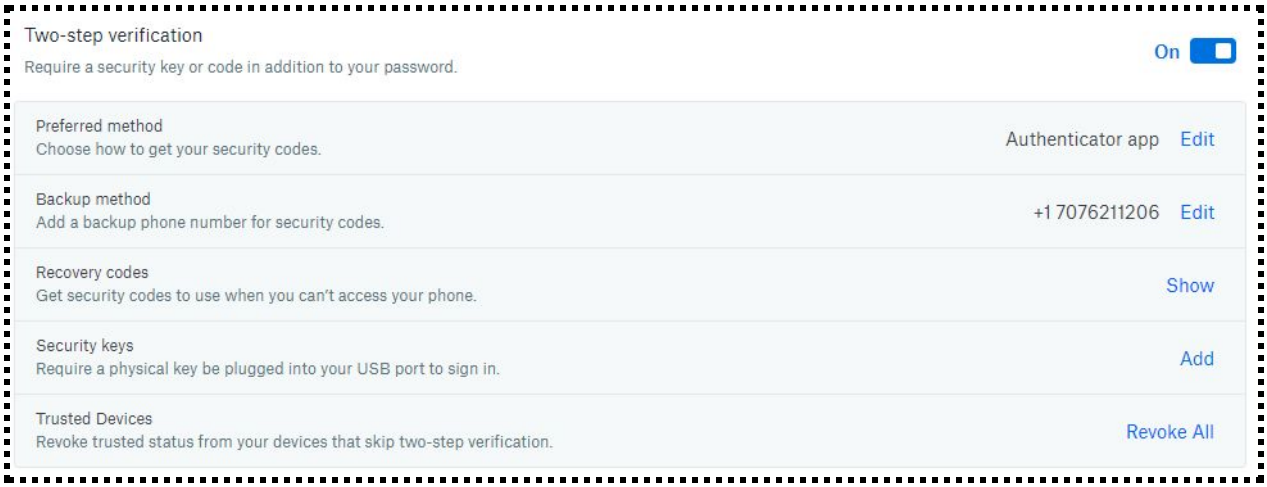
1. Email address verification
2. Devices and browsers
3. Linked Apps
4. Password Checkup
5. Check 2-Step Verification Settings

Review Recovery Codes

Click the Show link under Recovery Codes. Enter password again to continue. Look at the recovery codes, and make sure they are the same as what is in the Notes section of the Admin account's entry in LastPass. New codes don't need to be generated unless some of them have been used. *Note that this is only for individual accounts; it does not cover the organization as a whole.*

Review Two-Step Verification Settings

The settings should look like this:



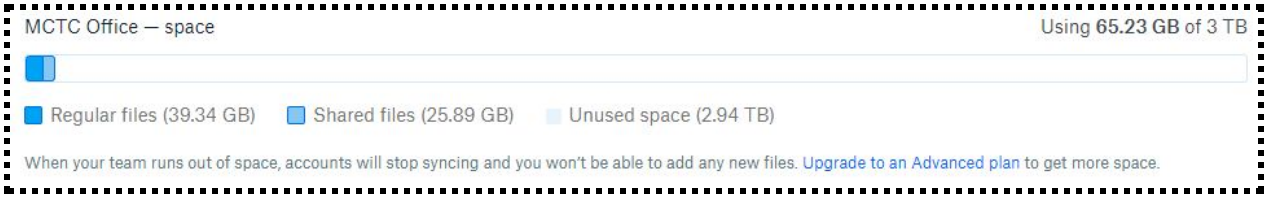
Revoke All Trusted Devices

Click the Revoke All link under Trusted Devices. This will force any device to prompt for two-step verification the next time Dropbox is used on that device.

Check Space Remaining

Under the General tab, make sure that Visit Mendocino County is not running out of space.

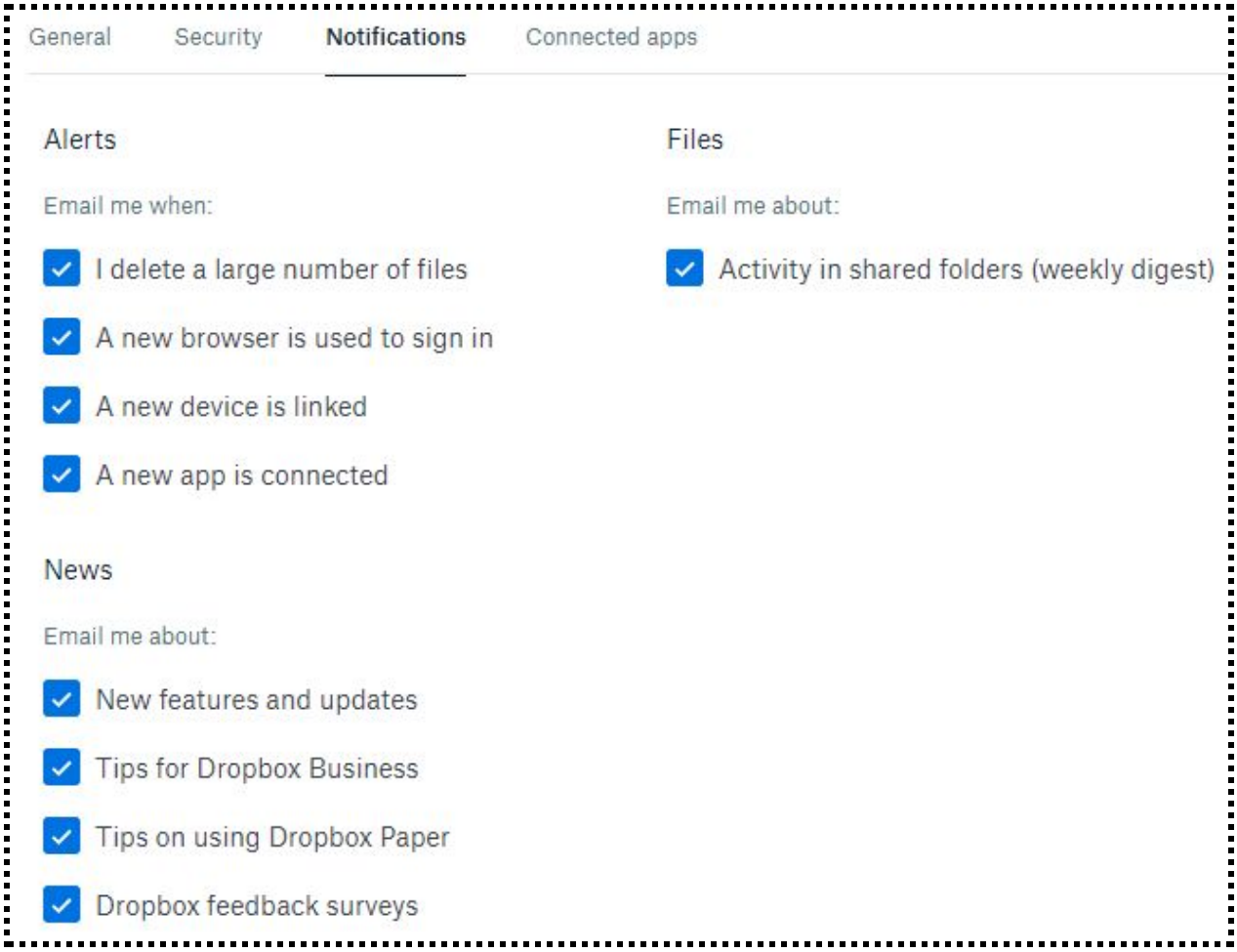
VMC Dropbox Storage Space 10/4/19: Using 65.23 GB of 3 TB



There is currently no problem with the amount of storage.

Check Notification Settings

Under the Notifications tab, make sure that all notifications are turned on like this:



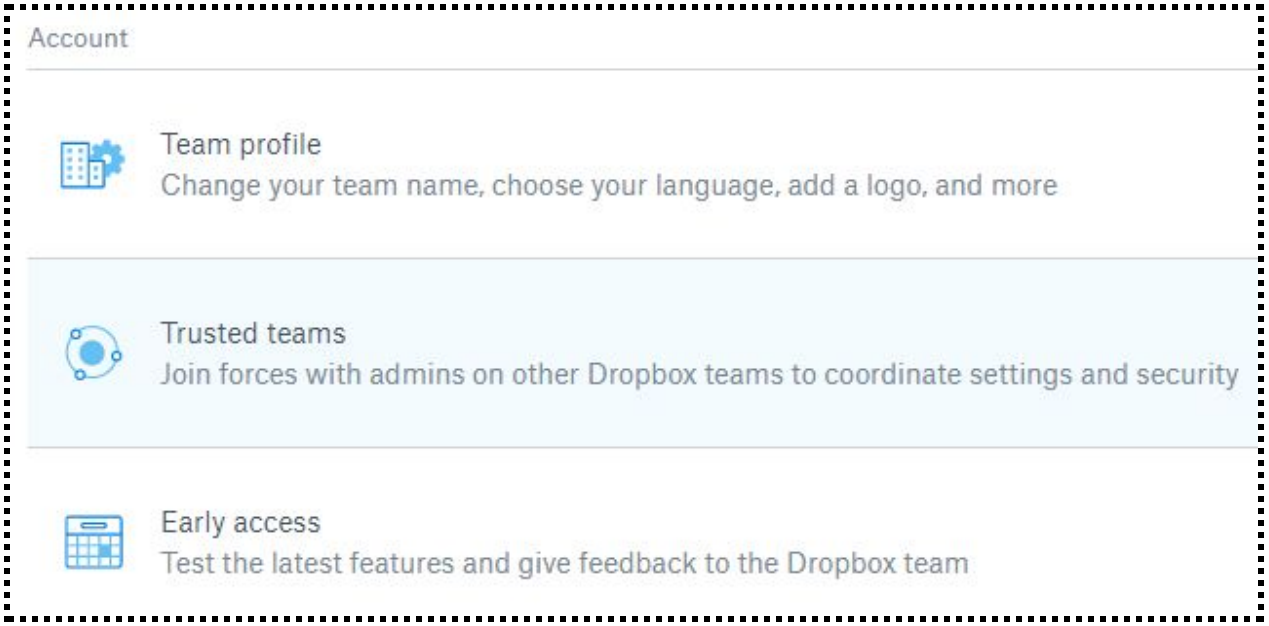
As of 10/4/19 all notifications are set correctly.

Dashboard: Usage

Review Active Members: as of 10/4/19 there are 10 active members.

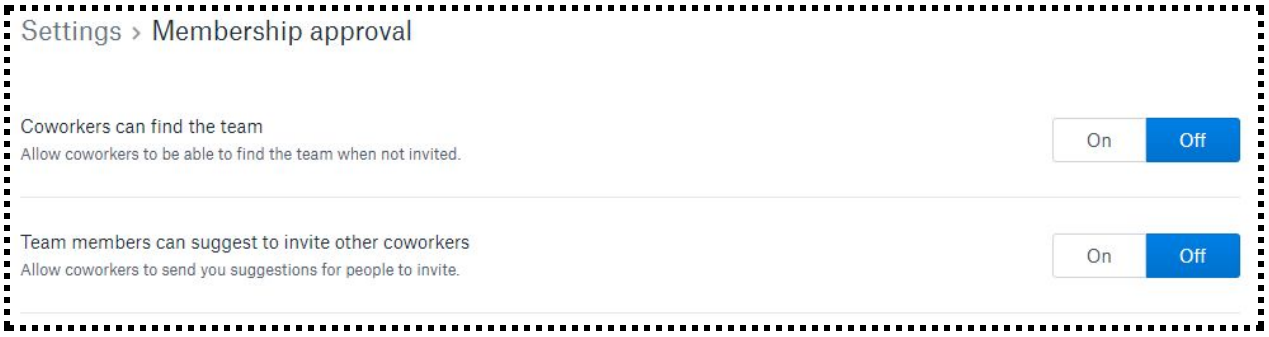
Review Active Devices: as of 10/4/19 there are currently 1 Windows, 6 MacOS, 2 iOS (9 total).

Review Trusted Teams: Under settings, make sure there are no trusted teams. A trusted team is a way for an external attacker to gain access to all aspects of Dropbox, and as of 10/4/19 there are no legitimate trusted teams added.



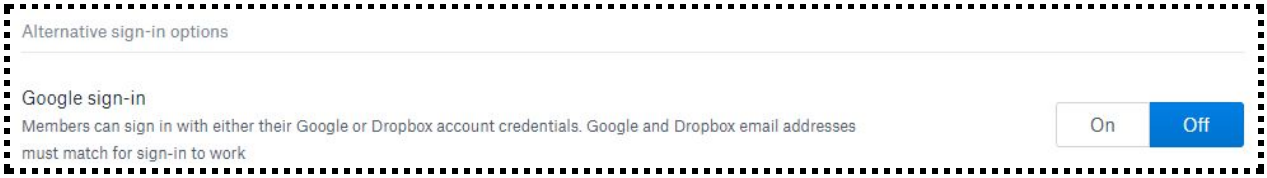
Review Membership Approval

Make sure both settings here are off. New members can only be added to VMC's Dropbox explicitly by an Admin account. Tom Jacobson turned both these settings to "Off" on 10/4/19. Prior that, both settings were set to "On."



Review Alternative Signon Methods

Under Settings, Single Signon, make sure that the option to sign in using Google credentials is turned OFF. Tom Jacobson turned both these settings to "Off" on 10/4/19. Prior that, both settings were set to "On." Tom Jacobson turned both this setting to "Off" on 10/4/19. Prior that, this settings was set to "On."



Download Dropbox Activity Report

Run an **activity report** for the last quarter. Make sure that all days since the last report was run are included. Run the report from the Activity tab. The report will show up in the Dropbox Business reports folder.

Review Dropbox Activity Report

Look through the report for entries where the name and/or email do not match a known VMC account. These are most often created when someone accesses a folder or file through Dropbox.

Here are some events to ask about:

On 10/02/19 the file VMC Q4 '19 Analytics .pptx was downloaded seven times through a link created by Allison de Grassi from Rio de Janeiro, Brazil, an Unknown location, Tokyo Japan, Georgetown, Maine, London, England, Las Vegas, Nevada, and Boardman, Oregon. No email addresses were associated with these file downloads, so it's not possible to tell who downloaded them.

2019-07-26T15:53:05+00:00 Sharing Invited non-team members to a shared folder 108.254.149.32 US San Francisco California laiko@keeferbahrspr.com laiko@keeferbahrspr.com {"orig_folder_name": "Robb Report", "shared_folder_id": "5977124480", "role": "viewer", "folder_name": "Robb Report", "host_id": 1, "emails": ["ko@kolicommunications.com"]}

GSuite Audit

Review Two-Step Verification

Google allows GSuite Admins to enforce Two-step verification (also known as two-factor authentication) for users. Visit Mendocino County does not currently require all users to use two-step verification. As of 10/04/19 only three users are using two-step verification: Travis, Ramon, and Tom. Visit Mendocino County should seriously consider enforcing two-step verification for all users by policy.

Review Admin Audit Log

On September 20th, 2019, Allison and Travis changed John Kuhry's GSuite account to become Jennifer Seward. The new email address is jennifer@visitmendocino.com. Because an existing account was changed, instead of an account being deleted and a new one being created, it's hard to know if this account is set up properly. For example, the new email address may still have John's old personal email and cell phone numbers as backups to recover the account. A full account review should be performed with Jennifer to make sure all of the information in her account is correct.

LastPass Audit

From an Admin account (Travis, Tom, Joh, Ramon) download the LastPass audit trail for the previous three months. Do this by going to the Admin Console: Reports: *** (menu item at top right): Export Report. Make sure to select the date range first!

Check for Suspicious Events

The main thing to look for are suspicious events in the LastPass audit trail. These are:

- New users added
- Old users removed
- Export of vault contents
- Accounts shared with people external to the organization
- Two-Factor Authentication (2FA) added / removed

As of 10/4/19, for the period from 07/01/2019 to 10/04/2019, there was only one event logged of any of the above types:

1. On August 29, 2019 at 10:10:18 AM a LastPass account for Emily was created. This was an expected event.

Check for Employee Usage

One red flag is if employees are not using LastPass. If an employee of Visit Mendocino County has a LastPass account but is not using it to log into accounts, that means they are using some other way of accessing those accounts - by using personal passwords (not unique / randomized passwords) or relying on a browser or some other program other than LastPass Teams to remember passwords.

As of 10/4/19, for the period from 07/01/2019 to 10/04/2019, not all employees are using LastPass on a daily and weekly basis to access sites. Kathy is not using LastPass at all, with the only record for her being on September 4, 2019 at 2:26:02 PM with a failed login attempt. Kathy is most likely using her computer's browsers to remember passwords and log in to sites. John Kuhry, a board member of Visit Mendocino County who has Administrative access to LastPass, has also not logged in at all during that time period.