

# WHAT TO DO

IF YOUR

0365

GSUITE

COMPUTER

IS  
HACKED.

# Who we are

---

Pine Cove Consulting created this eBook to help you if you believe your Microsoft 365, GSuite, or even computer has been hacked. if you are curious about what products and services we recommend to prevent cyber attacks, please reach out.



 **800.432.0346**

 **sales@pinecc.com**

# GSuite

1. Log into Google admin console. Find the compromised account.
2. Change password
3. Suspend account temporarily (only way to force sign-out of all sessions)
4. Determine if there are any account syncs that may be affected by the password change (manual investigation)

The screenshot displays the Google Admin console interface. At the top, there is a blue header with the 'Google Admin' logo, a search bar, and several utility icons. Below the header, the breadcrumb 'Users >' is visible, with a red circle containing the number '1' next to it. The main content area is divided into two columns. The left column shows the user's profile information, including a placeholder for a profile picture, the email address '@pinecc.com', and the status 'Active'. Below this, there is a list of actions: 'RESET PASSWORD' (with a red circle '2' next to it), 'UPDATE USER', 'UPLOAD PROFILE PHOTO', 'ADD ALTERNATE EMAILS', 'ADD TO GROUPS', 'EMAIL', and 'SUSPEND USER' (with a red circle '3' next to it). The right column contains three expandable sections: 'User information' (with a message about incomplete profile information), 'Security' (showing settings for 2-step verification, application-specific passwords, and connected applications), and 'Groups'. The overall layout is clean and professional, typical of a corporate management tool.

1. Reset sign in cookies
2. Investigate application-specific passwords & connected applications; remove anything the user doesn't recognize.
3. Investigate "signed in" devices; sign-out or delete suspicious devices
4. Enable account
5. Remote session w/ end-user "check things out."
6. Advise them to notify co-workers or other contacts (not via email)
7. Escalate to Pine Cove if needed/concerned

Users > [User Name]

**User information**

This user profile is incomplete. Add contact information for Cassie, like a secondary email address and a phone number.

**User details**

**Security** ← **click to expand**

2-step verification: OFF      Application-specific password

Not enforced and not enabled for [User Name]      0 application-specific passwords created

**Recovery information**

Email  
Add a recovery email

Phone  
Add a recovery phone

Recovery information is used to secure user accounts at sign-in and during account recovery.

**Require password change** OFF  
This password won't need to be changed once Cassie signs in.

**Login challenge**  
Turn off identity questions for 10 minutes after a suspicious attempt to sign in. [Learn more](#)

**2** **Sign in cookies**  
Resets the user's sign-in cookies, which also signs them out of their account across all devices and browsers.

**Application integrations**

**3** **Application-specific password**  
0 application-specific passwords. [Learn more](#)

**3** **Connected applications**  
2 applications connected to this user. [Learn more](#)

Devices > **Mobile and endpoints**

**1 device selected** ×

Status: All    + Add a filter

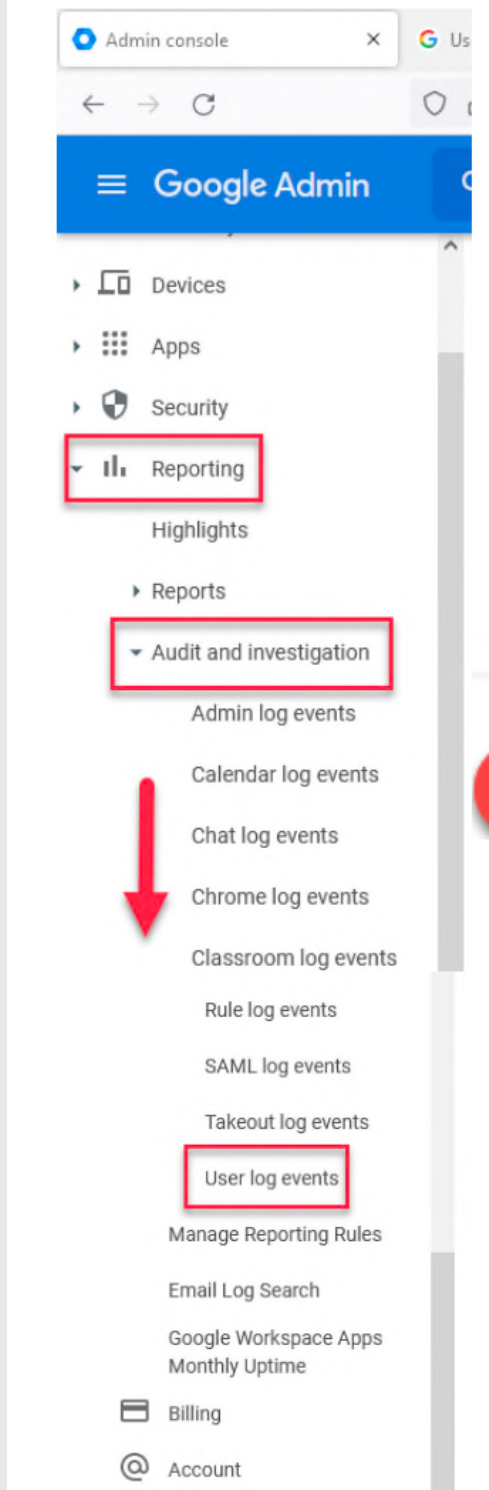
Device Name	Name	Email	OS	Ownership	First Sync	Last Sync ↓	Status
✓ Cassie's coral	Cassie Todd	ctodd@pinecc.com	Chrome OS 14526.69.0	User owned	61 days ago	15 hours ago	✓ Approved

**4**

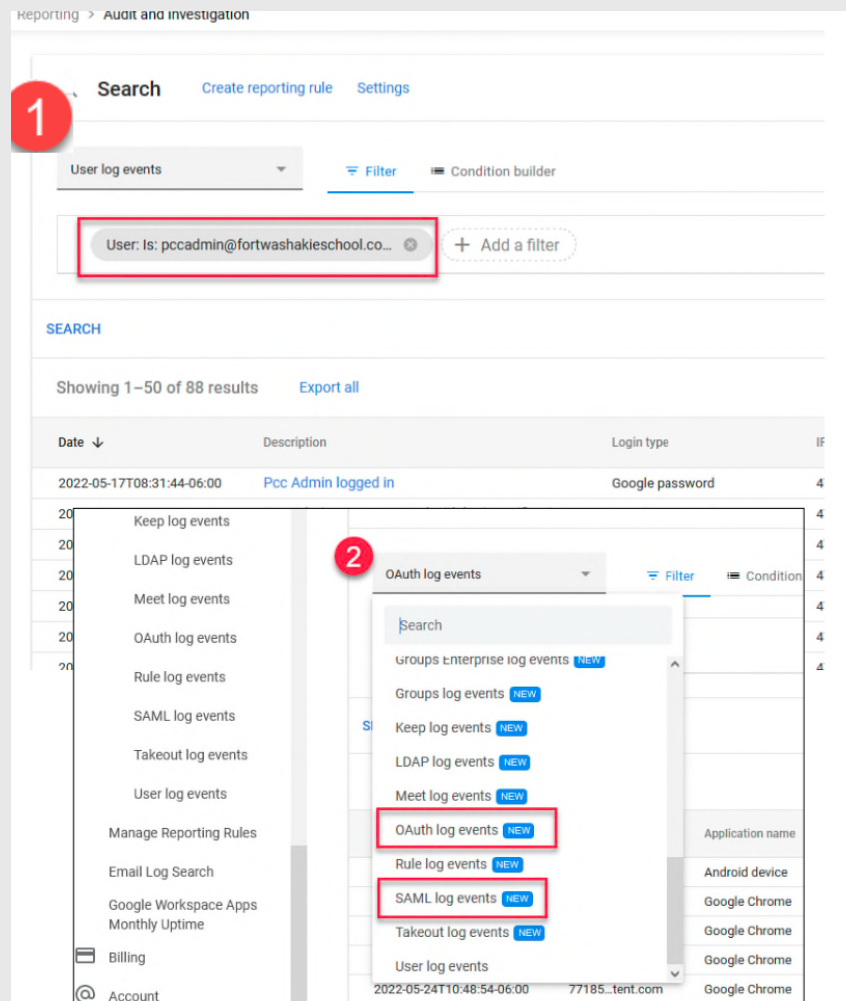
**SIGN OUT USER**

**DELETE DEVICES**

**VIEW AUDIT INFO**

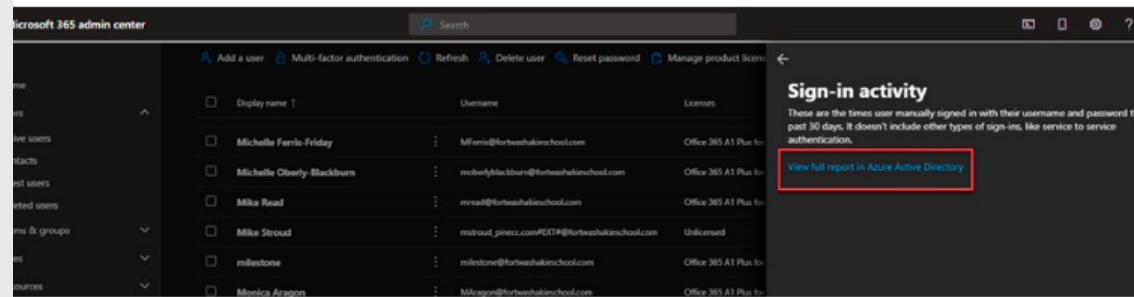
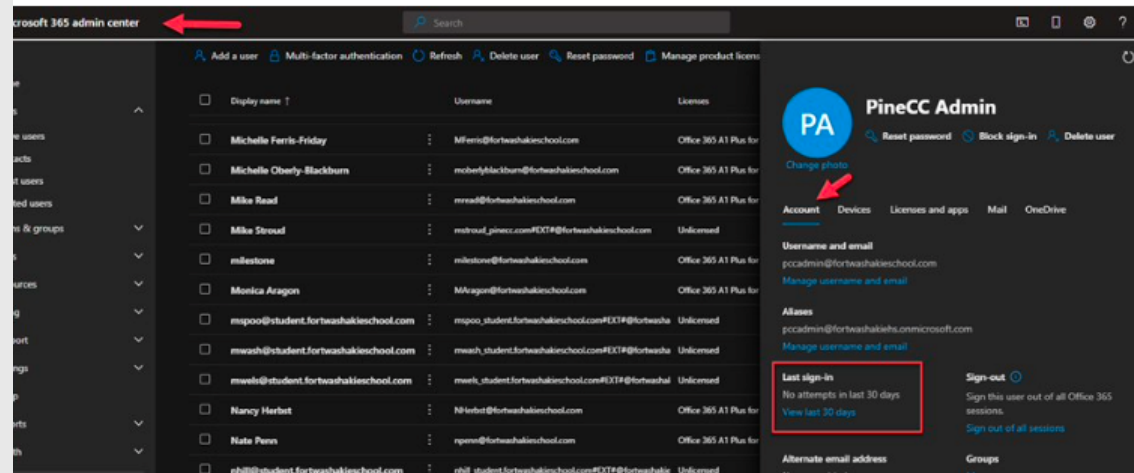
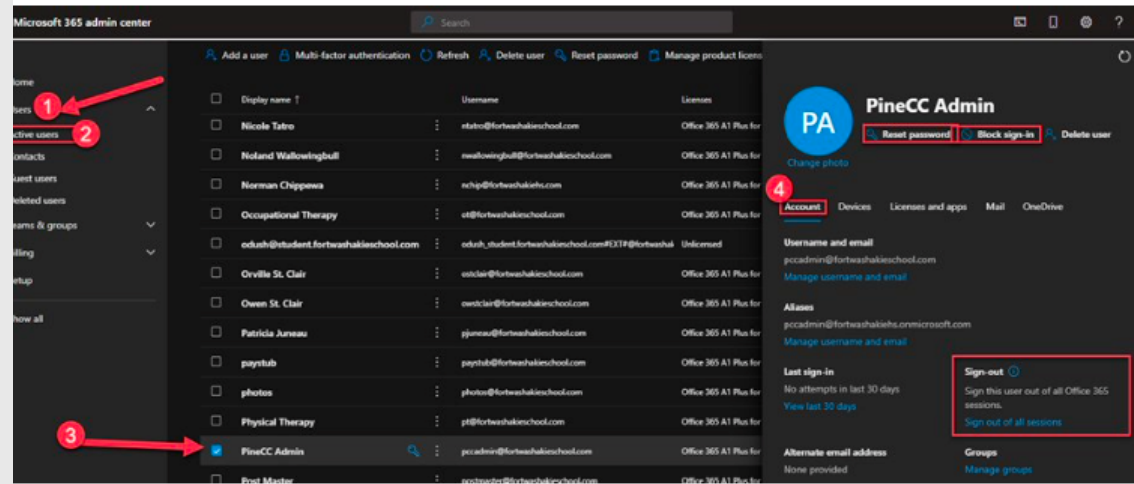


1. Use the Login Audit Log to view a complete list of successful & unsuccessful web-based sign-ins.
2. Look in the OAuth & SAML logs for suspicious sign-ins.
3. Enable account
4. Remote session w/ end-user to “check things out.”
5. Advise them to notify co-workers or other contacts (not via email)
6. Escalate to Pine Cove if needed/concerned

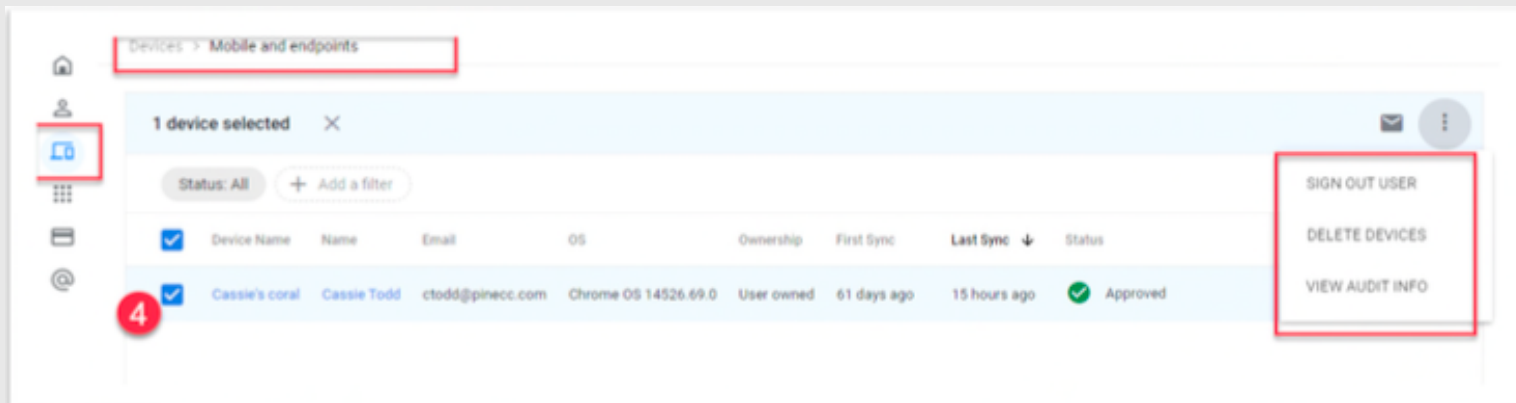
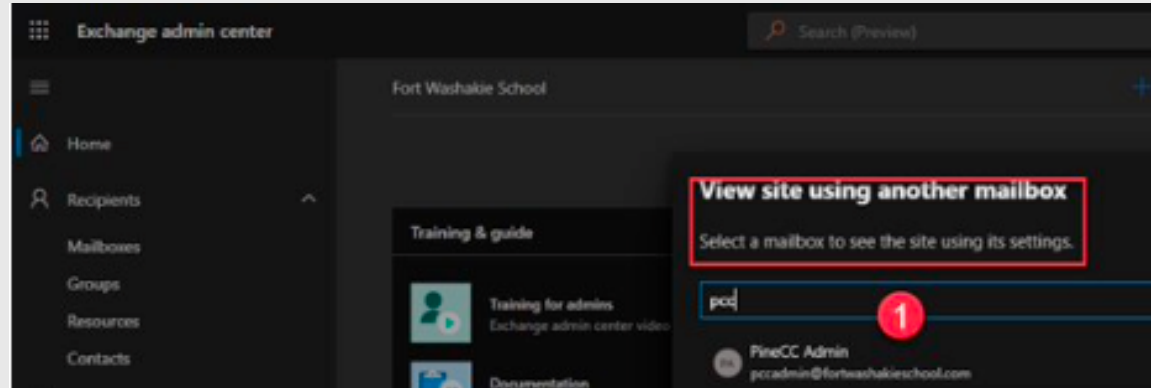
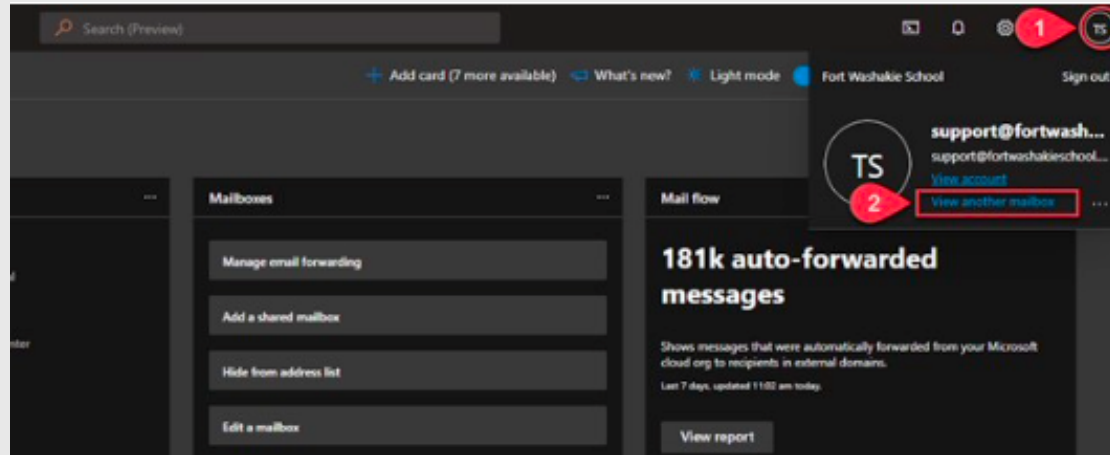


# 0365

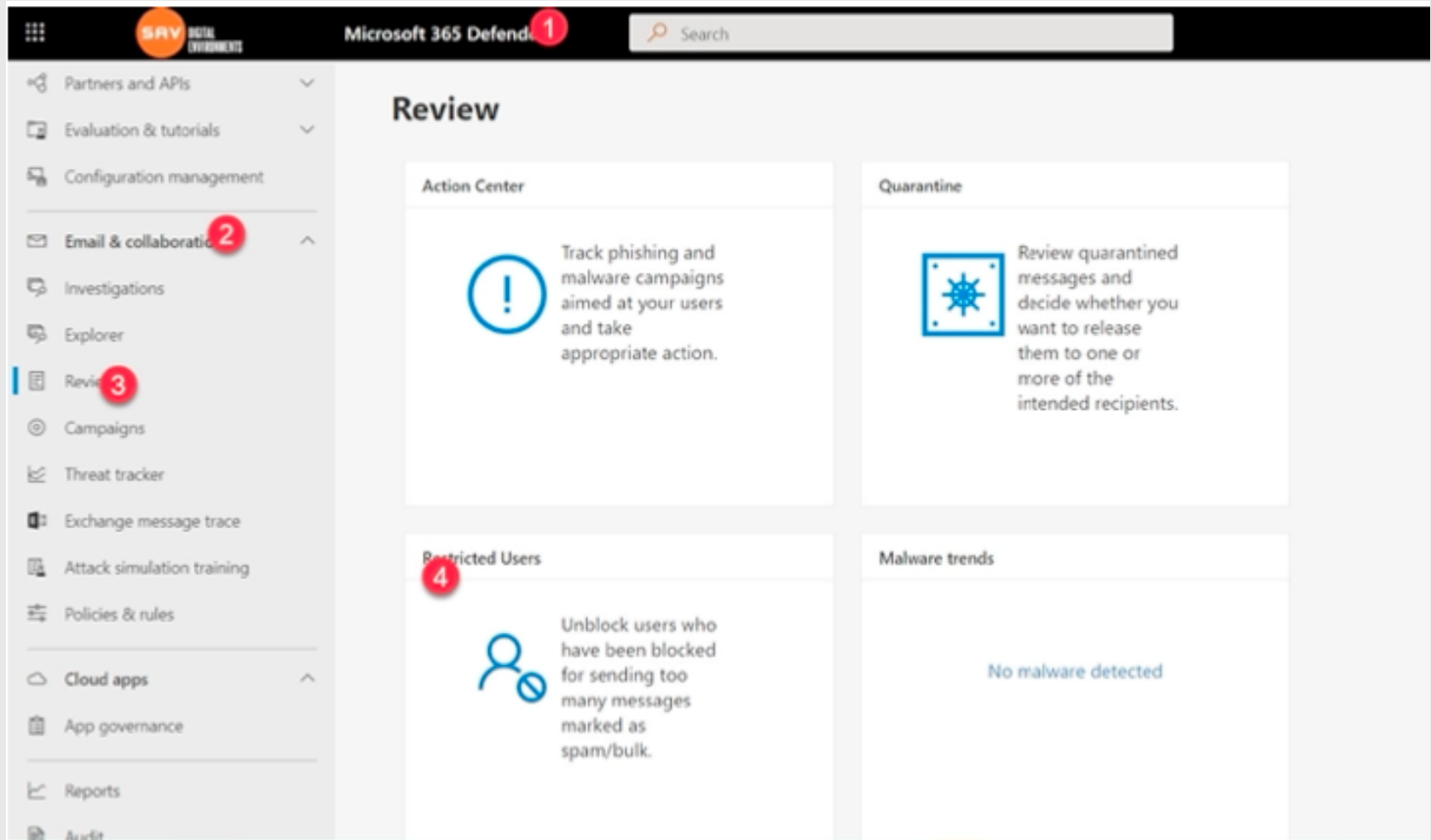
1. Log into 0365 admin console. Find a compromised account.
2. Change password
3. Sign out of all sessions
4. Check last sign-in info
5. Determine if there are any account syncs that may be affected by the password change (manual investigation)



1. Check for mailbox rules (OWA or O365 Admin)
2. Navigate to Exchange admin center
3. In top right, click on your user account and choose "view another account"
4. Type in the compromised account name
5. Once in the other account look for inbox rules. If any look suspicious, remove the rule.



1. Check to see if user is in "restricted users"(screenshot). Remove. Explain how/why if there
2. Remote session w/ end-user to "check things out"
3. Check for inbox rules(Outlook program)(screenshot)
4. Advise them to notify co-workers or other contacts (not via email)
5. Escalate to Pine Cove if needed/concerned



# Computer

1. Shut down computer
2. Coach end-user into booting into “safe mode without networking”
3. Coach end-user in removing cache, history, and unrecognized extensions (browser, check them all). (screenshot)
4. Coach end-user on uninstalling unrecognized or suspicious programs (look at install dates) (screenshot)
5. Boot normally (with networking) and check for functionality.
6. Virus scan (or install)
7. Change the password for the machine if applicable.
8. 7. Escalate to Pine Cove if needed/concerned

