pine cove
CONSULTING

WHAT TO DO

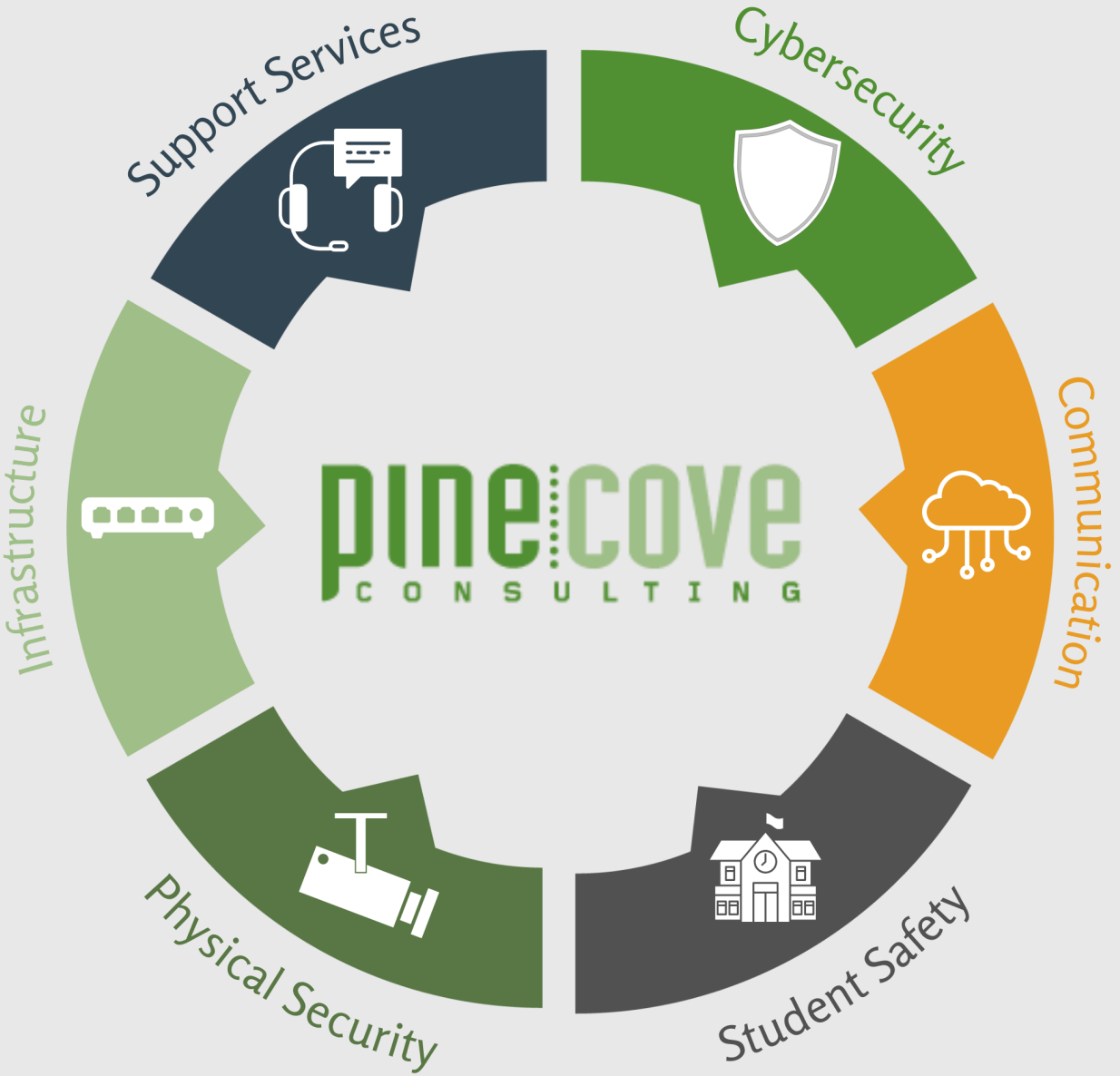
IF YOUR

O365
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.

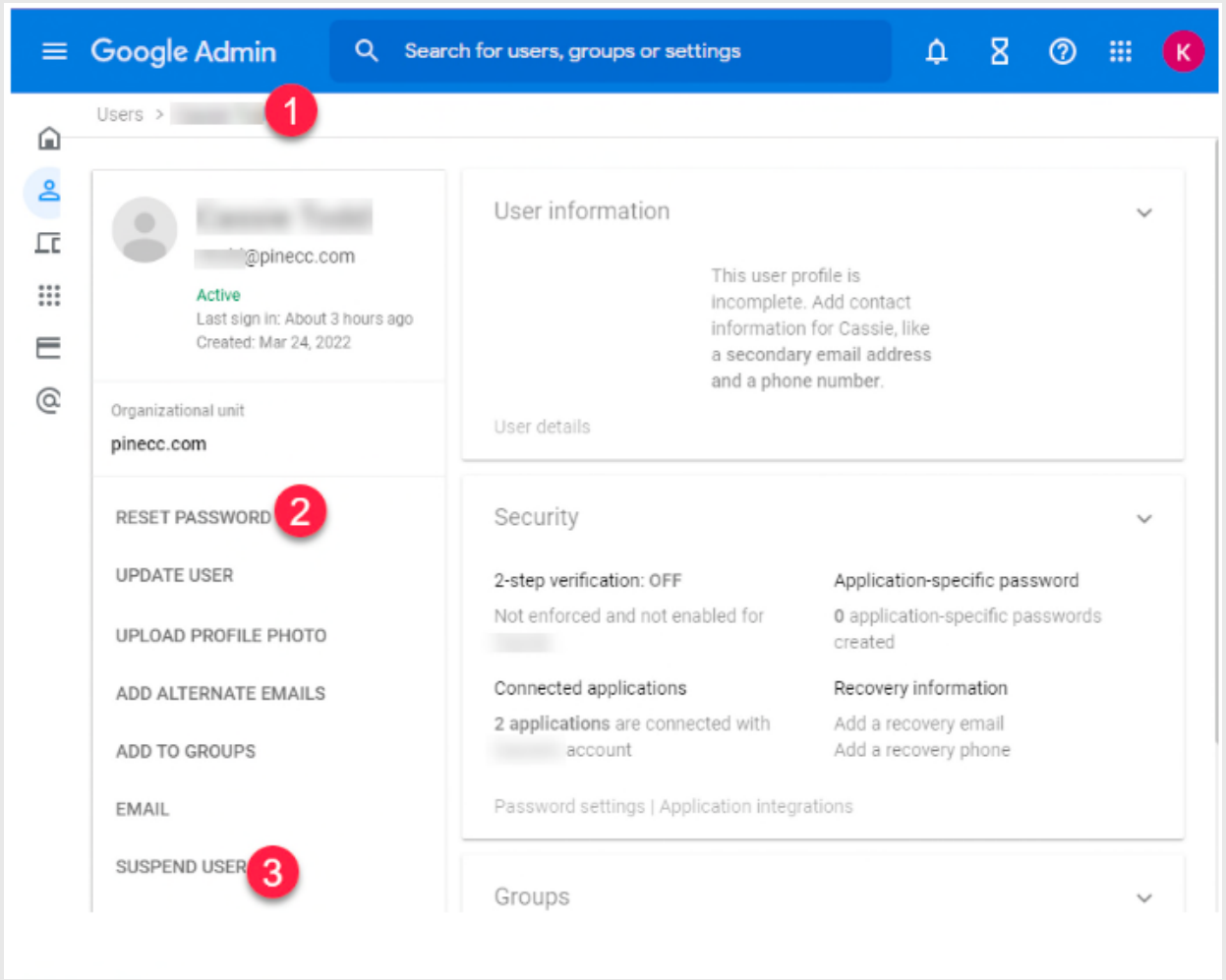


800.432.0346

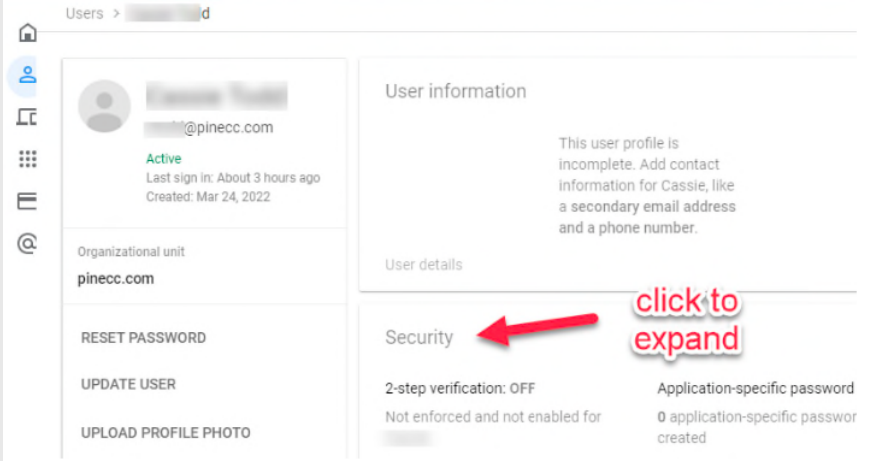
sales@pinecc.com

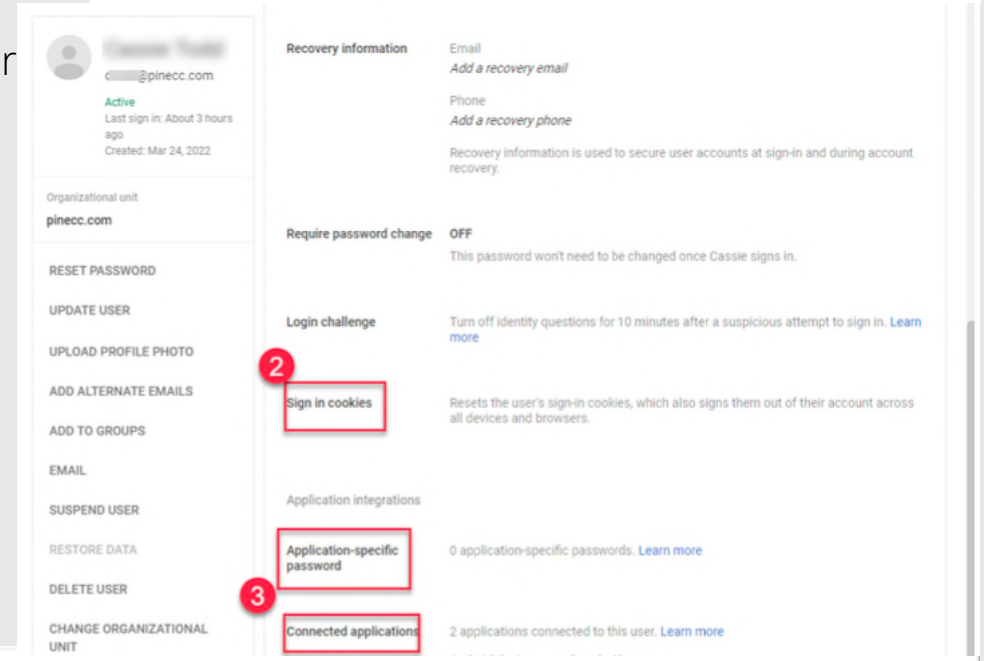
GSuite

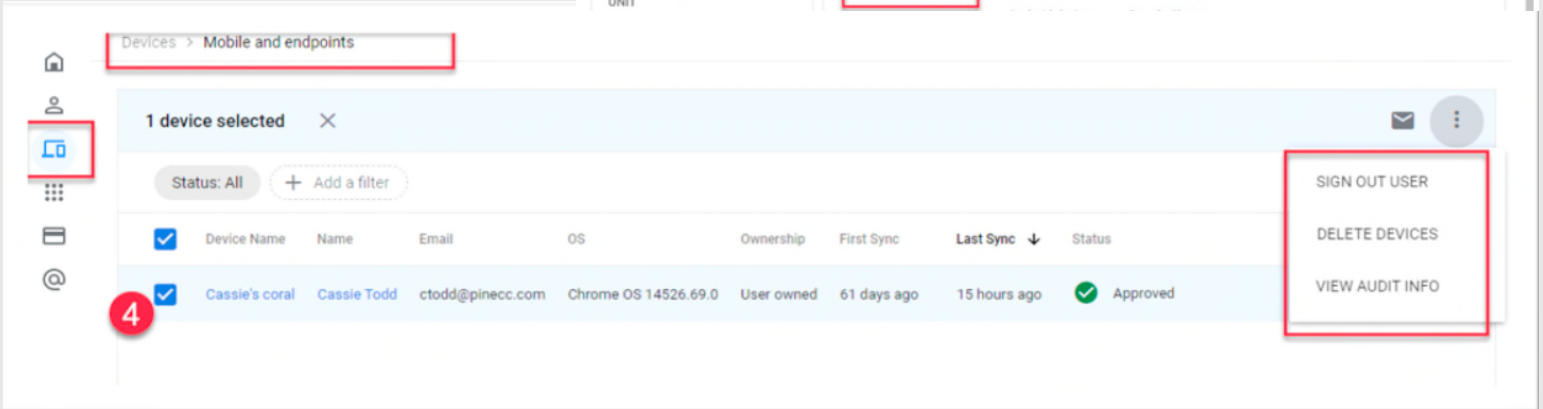
1. Log into Google admin console. Find the compromised account.
2. Change password
3. Suspend account temporarily (only way to force sign-out of all sessions)
4. Determine if there are any account syncs that may be affected by the password change (manual investigation)

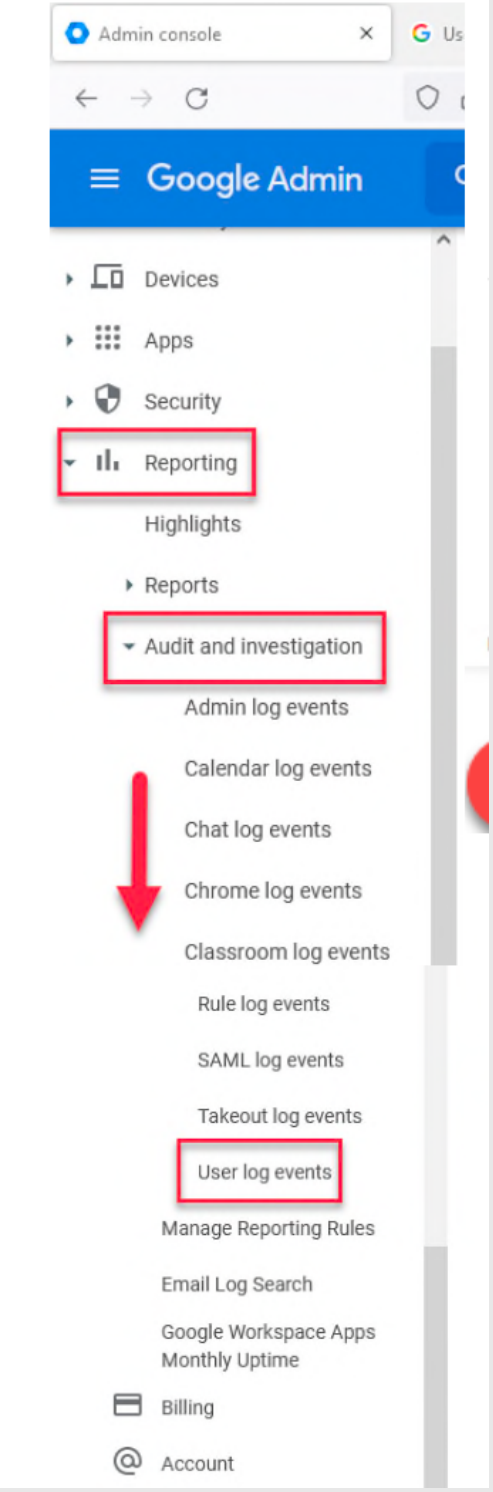


1. Reset sign in cookies
2. Investigate application-specific passwords & connected applications; remove anything the user doesn't recognize.
3. Investigate "signed in" devices; sign- out or delete suspicious devices
4. Enable account
5. Remote session w/ end-user "check things out."
6. Advise them to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

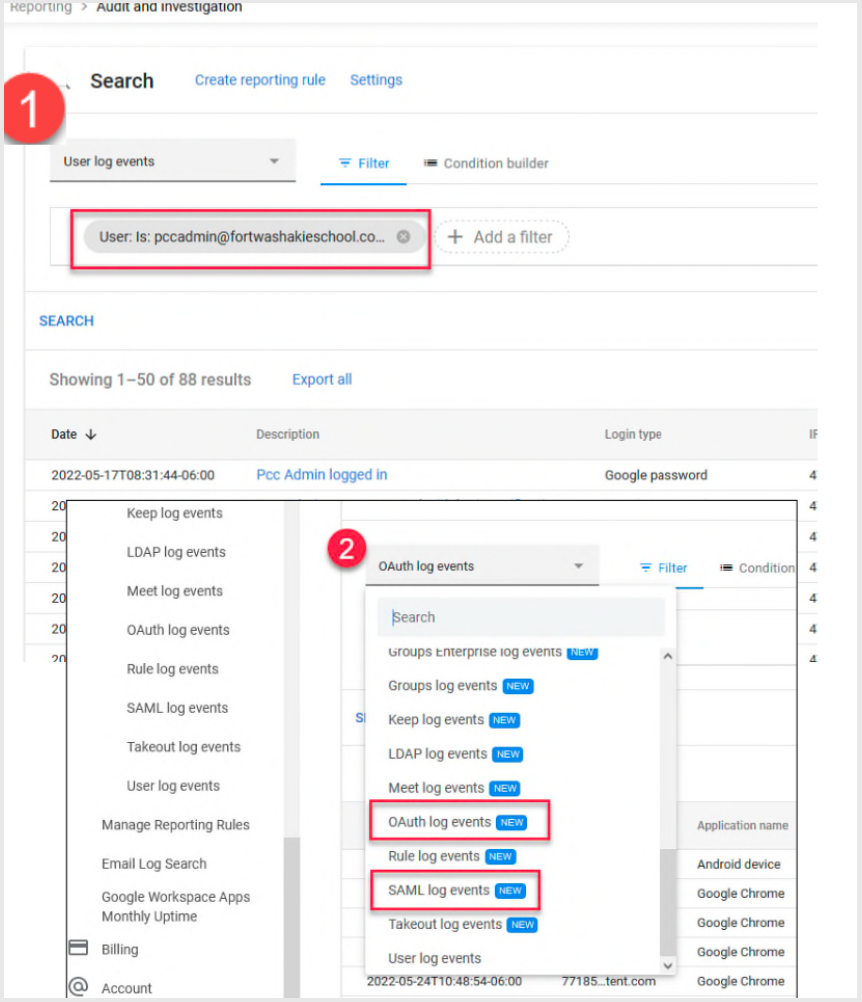






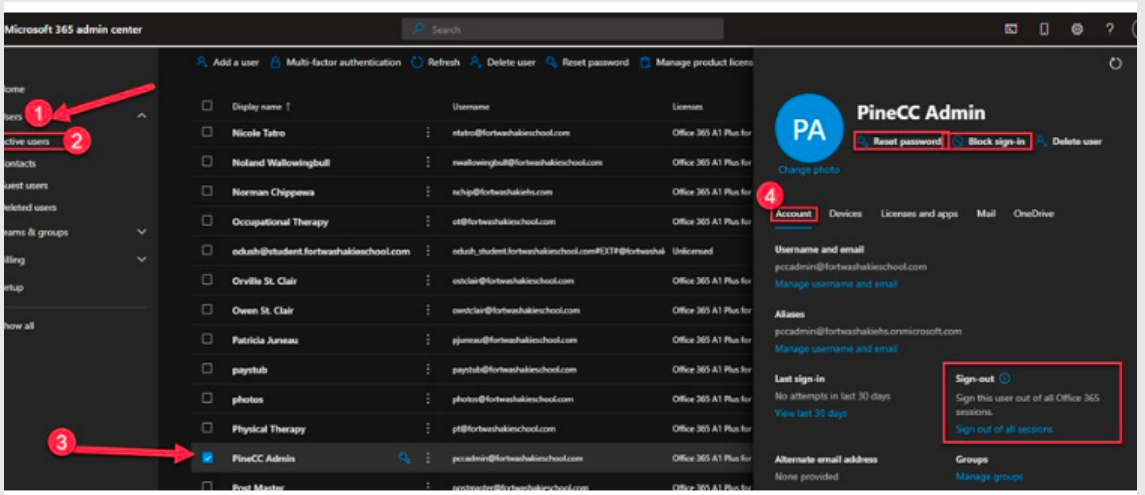


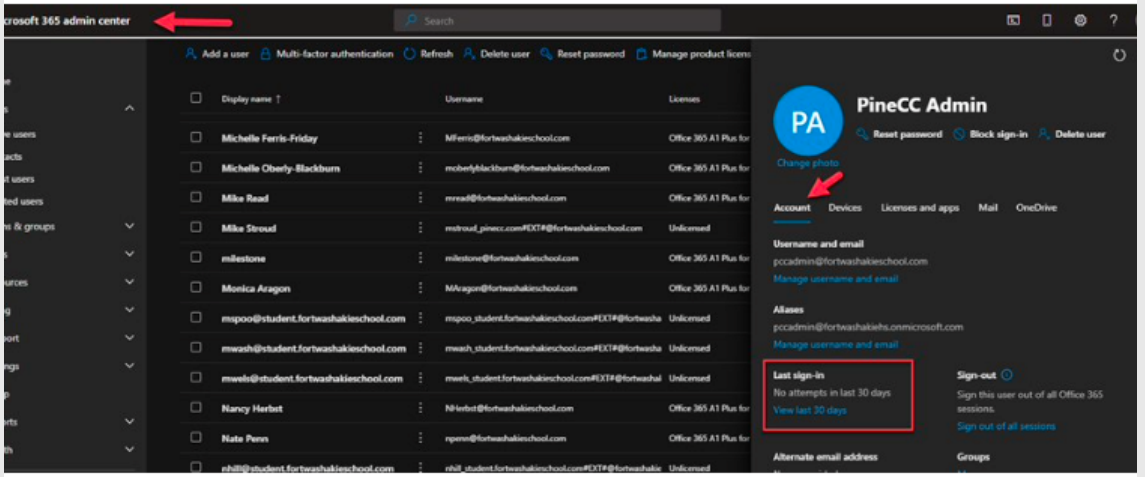
1. Use the Login Audit Log to view a complete list of successful & unsuccessful web-based sign-ins.
2. Look in the OAuth & SAML logs for suspicious sign-ins.
3. Enable account
4. Remote session w/ end-user to “check things out.”
5. Advise them to notify co-workers or other contacts (not via email)
6.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

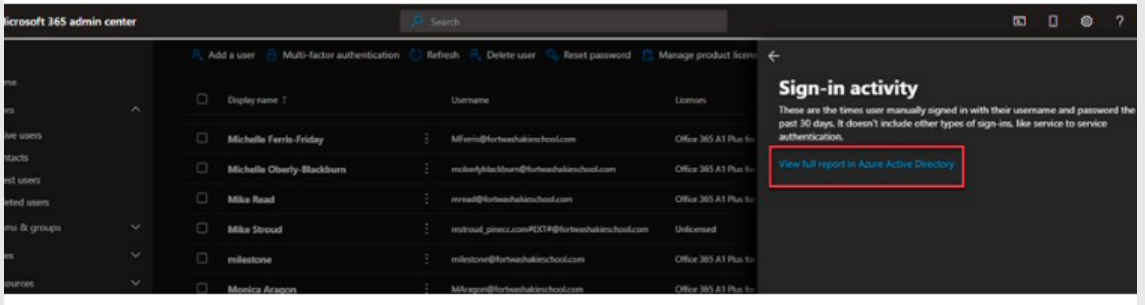


O365

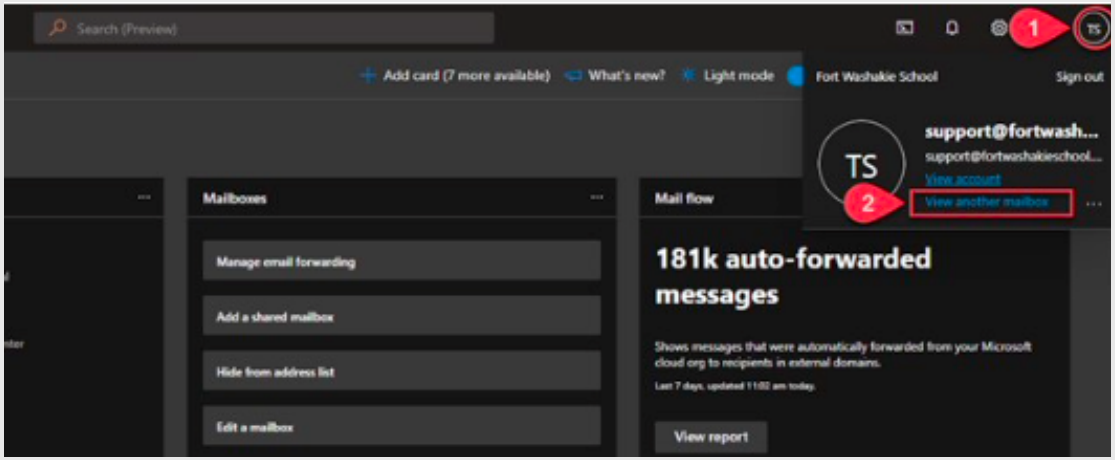
1. Log into 0365 admin console. Find a compromised account.
2. Change password
3. Sign out of all sessions
4. Check last sign-in info
5. Determine if there are any account syncs that may be affected by the password change(manual investigation)

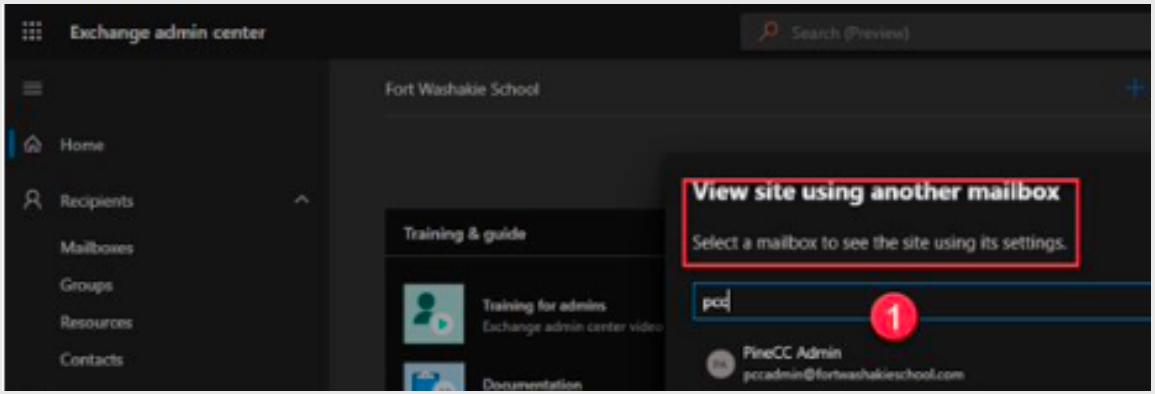


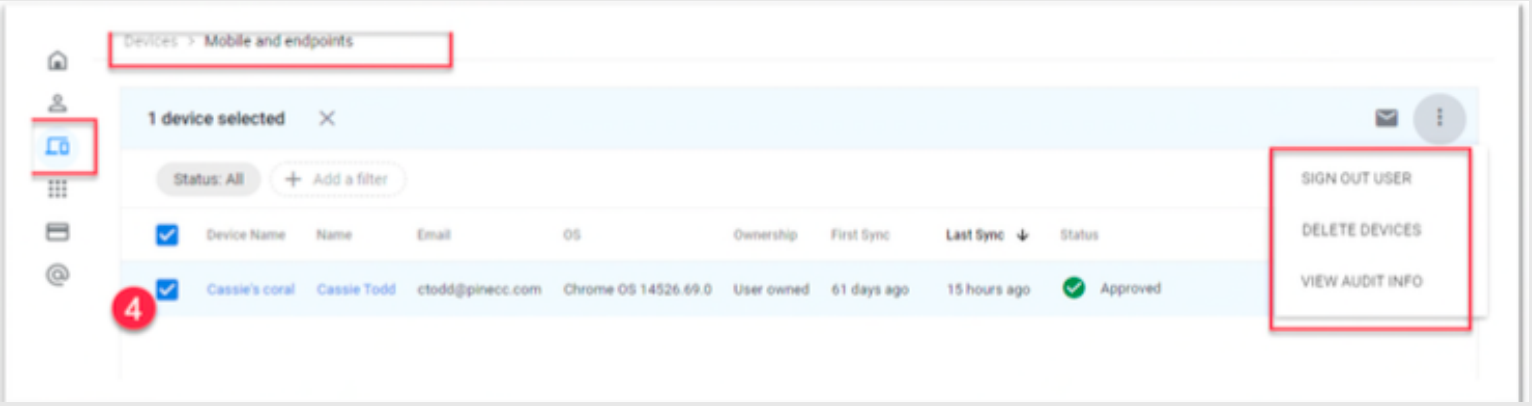




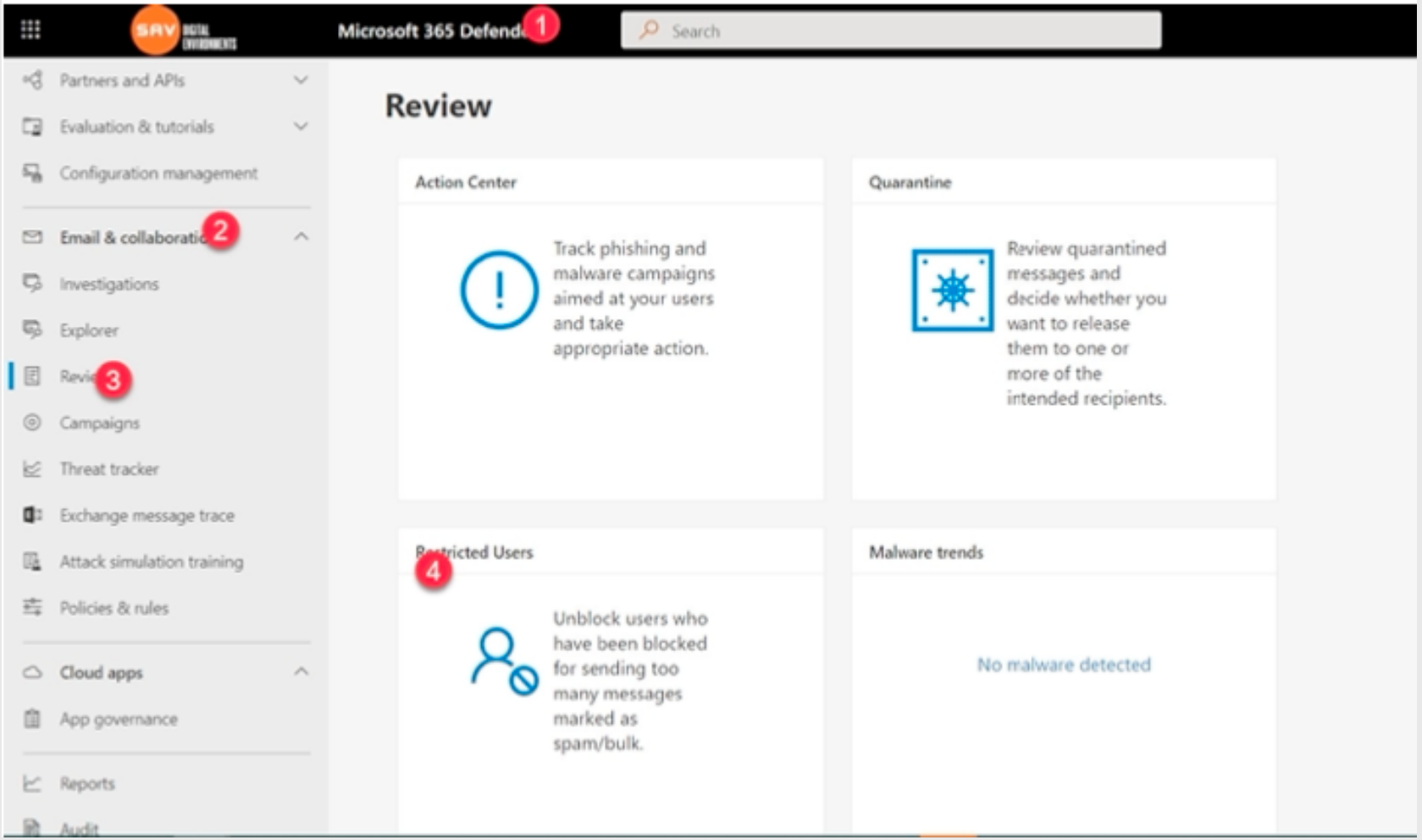
1. Check for mailbox rules (OWA or O365 Admin)
2. Navigate to Exchange admin center
3. In top right, click on your user account and choose "view another account"
4. Type in the compromised account name
5. Once in the other account look for inbox rules. If any look suspicious, remove the rule.







1. Check to see if user is in "restricited 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