

Safety

Can the client safely request and store the resulting export?

Goals:

1. Prevent the adversary from accessing the contents of the client's data export

2. Prevent the adversary from being notified that the client has requested their account data.

Checklist:

Ensure the client has a safe device that the adversary cannot physically access.

Check BOTH the target account and the primary email address associated with the account (if different) for compromise.

Are there unknown or malicious devices signed into the client's account?

Yes

Can the client safely sign out this device?

Could the adversary obtain authenticated access to the account?

Yes, via known credentials

Can the client safely change credentials or add MFA?

Yes, via recovery method

Can the client safely change the recovery method?

Yes, via physical access to client's devices

Can the client safely sign out of the shared device?

[For email accounts]
Is email forwarding set up?
If so, could the adversary access any of these emails?

Yes, appears compromised

Can the client safely disable email forwarding?

Ensure the client has the ability to re-authenticate the target account (knows password, has access to MFA)