EXECUTIVE PROTECTION

The Email That Recovers Your Accounts Needs a Way Back In

You try to open your email on a new computer. It asks you to approve the sign-in on the phone you have just lost. Recovering the phone account requires a message sent to that same inbox. Both accounts still exist, but neither lets you take the first step.

This situation develops quietly. You accept recovery options when you open services, then leave old numbers, unused addresses and retired devices attached for years. A strong password does not resolve a recovery process that depends on a single device.

Map the Dependencies Without Recording Secrets

Write down which email recovers each important account and where its second factor lives. Start with your main inbox, password manager and business administration accounts. The map should name owners and methods. It should never contain passwords or recovery codes.

- Check that you still control the registered addresses and numbers, without removing methods you currently need.
- Prepare a provider-supported alternative that does not depend entirely on your everyday phone.
- Keep recovery codes somewhere protected outside that device, where you can reach them if it goes missing.

Rehearse While the Working Route Stays Open

Review the official procedure on a second trusted computer while keeping a valid session. Do not wipe the phone or sign out everywhere to see what happens. The rehearsal should establish what the provider would ask for and where you would find it, without causing an actual lockout.

An executive protection review can reveal where personal accounts and business access depend on each other. Revisit the map after changing a number, an assistant or a device. Instructions left untouched for years are unlikely to reflect the accounts you use today.

Each provider sets its own recovery mechanisms and requirements. Preparing them reduces

dependence on one device, but does not guarantee recovery of a locked account.

A Check You Can Run

Try this paper exercise: cover the phone column in your recovery map and trace a route back to the main email account. If every route returns to that phone, the map has exposed a dependency. Record the provider-supported alternative and where its instructions are kept. Leave the working sign-in methods in place while you check it.

Supporting guidance: Google’s account recovery instructions.
https://support.google.com/accounts/answer/7682439

Continue with: A Password Manager Needs a Recovery Plan Too.
https://systems.kavaliero.com/en/blog/a-password-manager-needs-a-recovery-plan-too

For help with this work, see the scope of Executive Digital Protection.
https://systems.kavaliero.com/en/services/executive-security