

Recovery Codes & Backup Keys

When setting up two-factor authentication, most services provide one-time recovery codes. These are the "break glass" option if the authenticator app and security keys are both unavailable.

Where Recovery Codes Are Stored

[e.g., "Printed and stored in the fireproof safe," "Saved as a secure note in the password manager," "In a text file on the encrypted USB drive in the safe"]

Recovery Codes by Service

Service	Recovery Codes Location	Notes
Google	<i>[Location]</i>	

Apple ID	<i>[Location]</i>	<i>[Recovery key? Trusted phone number?]</i>
Microsoft	<i>[Location]</i>	
Password Manager	<i>[Location]</i>	<i>[Most critical one]</i>
<i>[Other critical service]</i>	<i>[Location]</i>	

Encrypted USB / Backup Drive

[If you keep recovery codes or sensitive files on an encrypted USB drive, where is it and what's the decryption password?]

Location	<i>[Where the USB drive is]</i>
Encryption Method	<i>[e.g., BitLocker, VeraCrypt]</i>
Password	<i>[Where to find it]</i>