PREVENTIVE PREPARATION

Documents to Save NOW (Before Disaster)

1. Rclone Configuration

```
# Backup rclone configuration
rclone config show > ~/Desktop/rclone-config-backup.txt
```

Save this file in:

- Password manager (as secure note)
- Offline USB drive

SCENARIO 1: ACCIDENTAL FILE DELETION

Problem: You deleted an important file (yesterday or last week)

Step 1: Find the file

```
# Search in all snapshots
restic -r rclone:gdrive_union:/restic-backup find "filename.pdf"
```

Example output:

```
repository a1b2c3d4 opened successfully, password is correct
Found matching entries in snapshot 1a2b3c4d from 2025-11-02 10:30:00
  /Users/<your-username>/Desktop/filename.pdf

Found matching entries in snapshot 5e6f7g8h from 2025-10-28 14:20:00
  /Users/<your-username>/Desktop/filename.pdf
```

Step 2: Choose snapshot and restore

```
# Restore from most recent snapshot
restic -r rclone:gdrive_union:/restic-backup restore 1a2b3c4d \
```

```
  --target ~/Desktop/recovery \
  --include /Users/<your-username>/Desktop/filename.pdf
```

Step 3: Verify and copy

```
# Recovered file will be in:
ls ~/Desktop/recovery/Users/<your-username>/Desktop/filename.pdf

# Copy to original location
cp ~/Desktop/recovery/Users/<your-username>/Desktop/filename.pdf ~/Desktop/

# Verify it's ok
open ~/Desktop/filename.pdf

# Cleanup
rm -rf ~/Desktop/recovery
```

SCENARIO 2: RECOVERING PREVIOUS FILE VERSION

Problem: You modified a file and want the version from 2 weeks ago

Step 1: Find all versions

```
# Search file and show all snapshots containing it
restic -r rclone:gdrive_union:/restic-backup find "project.docx"
```

Example output:

```
Found matching entries in snapshot 1a2b3c4d from 2025-11-02 10:30:00
Found matching entries in snapshot 5e6f7g8h from 2025-10-25 09:15:00
Found matching entries in snapshot 9i0j1k2l from 2025-10-18 11:00:00
Found matching entries in snapshot 3m4n5o6p from 2025-10-11 10:45:00
```

Step 2: Restore desired version

```
# Restore October 18 version
restic -r rclone:gdrive_union:/restic-backup restore 9i0j1k2l \
  --target ~/Desktop/previous-versions \
  --include /Users/<your-username>/Desktop/project.docx
```

Step 3: Compare versions

```
# Compare with current version
diff ~/Desktop/project.docx ~/Desktop/previous-versions/Users/<your-
username>/Desktop/project.docx
```

SCENARIO 3: CORRUPTION/RANSOMWARE

Problem: Files corrupted or encrypted by malware, need to return to a "clean" snapshot

Step 1: STOP - Don't make additional backups

```
# IMPORTANT: Disable automatic backup IMMEDIATELY
launchctl unload ~/Library/LaunchAgents/com.user.restic-backup.plist

# Verify it's stopped
launchctl list | grep restic
# If nothing appears = it's stopped
```

Step 2: Identify the last clean snapshot

```
# List all snapshots with dates
restic -r rclone:gdrive_union:/restic-backup snapshots
```

Reason about the timeline:

- When did you notice the problem? (e.g., today November 2 at 2:00 PM)
- When did you last use the files without issues? (e.g., yesterday November 1 at 6:00 PM)
- Safe snapshot: the one from November 1 at 5:00 PM

Step 3: Verify clean snapshot

```
# List files in suspect snapshot (today's)
restic -r rclone:gdrive_union:/restic-backup ls latest | head -20

# List files in clean snapshot (yesterday's)
restic -r rclone:gdrive_union:/restic-backup ls <clean-snapshot> | head -20
```

```
# Compare to see differences
restic -r rclone:gdrive_union:/restic-backup diff <clean-snapshot> latest
```

Output will show you:

- `M` = modified files (suspect if encrypted)
- `+` = new files (could be malware)
- `-` = deleted files (could have been replaced)

Step 4: Full restore from clean snapshot

```
# BACKUP CURRENT (even if corrupted) for forensic analysis
mkdir ~/Desktop/INFECTED-BACKUP
cp -R ~/Desktop/* ~/Desktop/INFECTED-BACKUP/

# Restore from clean snapshot
restic -r rclone:gdrive_union:/restic-backup restore <clean-snapshot> \
  --target ~/Desktop/RECOVERY-CLEAN

# Verify recovered files
ls ~/Desktop/RECOVERY-CLEAN/Users/<your-username>/Desktop/
```

Step 5: Verify recovered file integrity

```
# Test opening file
open ~/Desktop/RECOVERY-CLEAN/Users/<your-username>/Desktop/document.pdf

# Re-enable backup
launchctl load ~/Library/LaunchAgents/com.user.restic-backup.plist
```

Step 6: Cleanup infected snapshots

```
# Identify infected snapshots
restic -r rclone:gdrive_union:/restic-backup snapshots

# Delete infected snapshots
restic -r rclone:gdrive_union:/restic-backup forget <infected-snapshot-1>
<infected-snapshot-2> --prune

# Verify
restic -r rclone:gdrive_union:/restic-backup snapshots
```

Estimated time: 30-60 minutes

SCENARIO 4: COMPLETE MAC LOSS

Problem: Mac stolen, disk broken, or need to start from scratch on new Mac

Step 1: Setup new Mac

```
# Install Restic and Rclone
brew install restic rclone
```

Step 2: Reconfigure Rclone remotes

OPTION A: If you have rclone.conf backup

```
# Restore configuration
mkdir -p ~/.config/rclone
cp /path/to/backup/rclone-backup.conf ~/.config/rclone/rclone.conf

# Test connections
rclone lsd gdrive1:
rclone lsd gdrive2:
rclone lsd gdrive3:
rclone lsd mega1:
rclone lsd mega2:
```

OPTION B: Reconfigure manually (follow Phase 2 from original guide)

```
rclone config

# For EACH remote (gdrive1, gdrive2, gdrive3, mega1, mega2):
# - n = new remote
# - Name: gdrive1 (then gdrive2, gdrive3, mega1, mega2)
# - Type: 22 (Google Drive) or 35 (MEGA)
# - Scope: 1
# - Web browser authentication: y
# - Team Drive: n

# After creating all 5 remotes, create the unions:
rclone config create gdrive_union union upstreams "gdrive1: gdrive2:
gdrive3:"
rclone config create mega_union union upstreams "mega1: mega2:"
```

```
# Verify unions
rclone lsd gdrive_union:
rclone lsd mega_union:
```

Step 3: Recover Restic password

```
# From your password manager, recover password "Restic-Rclone"
# Set it as environment variable for this session
export RESTIC_PASSWORD="your-30-character-password"
```

Step 4: Verify repository

```
# Verify primary repository
restic -r rclone:gdrive_union:/restic-backup snapshots

# Verify mirror repository
restic -r rclone:mega_union:/restic-backup snapshots

# Quick integrity check
restic -r rclone:gdrive_union:/restic-backup check
```

Step 5: Full restore

```
# List available snapshots
restic -r rclone:gdrive_union:/restic-backup snapshots

# Restore last complete snapshot
restic -r rclone:gdrive_union:/restic-backup restore latest \
  --target ~/Desktop \
  --verbose
```

Step 6: Verify restore

```
# Check sizes
du -sh ~/Desktop

# Verify critical files
ls ~/Desktop/Memories/
```

Step 7: Reinstall automation

```
# Recreate scripts directory
mkdir -p ~/.local/share/restic-backup/{Scripts,logs}

# Copy scripts (backup-desktop.sh and verify-repositories.sh)
# from your original guide or from backup

# Add password to Keychain
security add-generic-password \
  -a "$USER" \
  -s "restic-backup" \
  -w "your-30-character-password"

# Recreate LaunchAgent
nvim ~/Library/LaunchAgents/com.user.restic-backup.plist
# Copy content from original guide

# Load job
launchctl load ~/Library/LaunchAgents/com.user.restic-backup.plist
launchctl list | grep restic
```

SCENARIO 5: PRIMARY REPOSITORY CORRUPTION

Problem: Google Drive has issues, primary repository corrupted

Step 1: Diagnosis

```
# Attempt check on primary repository
restic -r rclone:gdrive_union:/restic-backup check

# If errors, attempt check on mirror
restic -r rclone:mega_union:/restic-backup check
```

If mirror is OK → proceed with recovery

Step 2: Use mirror as temporary primary

```
# All commands now point to MEGA
export RESTIC_REPOSITORY="rclone:mega_union:/restic-backup"

# Verify it works
```

```
restic snapshots
restic check
```

Step 3: Restore from mirror

```
# Normal restore from MEGA
restic restore latest --target ~/Desktop/recovery-from-mega
```

Step 4: Rebuild Google repository

```
# Option A: Repair existing repository
restic -r rclone:gdrive_union:/restic-backup rebuild-index
restic -r rclone:gdrive_union:/restic-backup prune
restic -r rclone:gdrive_union:/restic-backup check

# If Option A fails → Option B: Reinitialize
# WARNING: deletes everything on Google Drive
rclone purge gdrive_union:/restic-backup

# Reinitialize repository
restic -r rclone:gdrive_union:/restic-backup init

# Copy all snapshots from MEGA to Google
restic -r rclone:mega_union:/restic-backup copy \
  --repo2 rclone:gdrive_union:/restic-backup

# Verify
restic -r rclone:gdrive_union:/restic-backup check
restic -r rclone:gdrive_union:/restic-backup snapshots
```

SCENARIO 6: BOTH REPOSITORIES CORRUPTED

Problem: Both Google Drive and MEGA have issues (WORST CASE)

Step 1: Damage analysis

```
# Check primary repository
restic -r rclone:gdrive_union:/restic-backup check 2>&1 | tee gdrive-
check.log

# Check mirror repository
```

```
restic -r rclone:mega_union:/restic-backup check 2>&1 | tee mega-check.log

# Analyze logs to understand severity
cat gdrive-check.log
cat mega-check.log
```

Step 2: Attempt automatic repair

```
# Attempt rebuild index on both
restic -r rclone:gdrive_union:/restic-backup rebuild-index
restic -r rclone:mega_union:/restic-backup rebuild-index

# Attempt prune
restic -r rclone:gdrive_union:/restic-backup prune
restic -r rclone:mega_union:/restic-backup prune

# Re-check
restic -r rclone:gdrive_union:/restic-backup check
restic -r rclone:mega_union:/restic-backup check
```

Step 3: Partial recovery

Even if repositories are corrupted, **some snapshots might be recoverable:**

```
# List existing snapshots (even if repository damaged)
restic -r rclone:gdrive_union:/restic-backup snapshots

# Attempt restore from most recent intact snapshot
restic -r rclone:gdrive_union:/restic-backup restore <last-good-snapshot> \
  --target ~/Desktop/emergency-recovery
```

Step 4: Manual data packs recovery

Direct access to packs:

```
# List available packs
restic -r rclone:gdrive_union:/restic-backup list packs

# Mount repository (even if partially corrupted)
mkdir ~/restic-mount
restic -r rclone:gdrive_union:/restic-backup mount ~/restic-mount --allow-
other
```

```
# Navigate and manually copy recoverable files
cp -R ~/restic-mount/snapshots/<snapshot-id>/* ~/Desktop/manual-recovery/
```

Step 5: Future prevention

If this happens, it means you need a **3rd redundancy repository:**

```
# Add third provider (e.g., Dropbox)
rclone config # configure dropbox

# Initialize new repository
restic -r rclone:dropbox:/restic-backup init

# From now on, backup to 3 repositories
restic -r rclone:gdrive_union:/restic-backup backup ~/Desktop
restic -r rclone:mega_union:/restic-backup backup ~/Desktop
restic -r rclone:dropbox:/restic-backup backup ~/Desktop
```

SCENARIO 7: RESTIC PASSWORD LOSS

Problem: You lost the Restic repository password

What to do

1. **Search everywhere:**
   - Password manager (search "Restic", "Rclone", "Backup")
   - Email (search "restic password")
   - Phone notes
   - Secure notes
   - Physical printouts

Prevention

```
# NOW add second recovery key
restic -r rclone:gdrive_union:/restic-backup key add

# Save this second password in different location:
# - Sealed envelope in safe
# - Different password manager
# - Bank safe deposit box
```

SCENARIO 8: CLOUD CREDENTIALS LOSS

Problem: You lost access to Google Drive or MEGA accounts

Google Drive recovery

```
# 1. Recover Google account access
# - Go to accounts.google.com/recovery
# - Use recovery email/phone
# - Follow password reset procedure

# 2. Once back in, reconfigure rclone
rclone config reconnect gdrive1:
rclone config reconnect gdrive2:
rclone config reconnect gdrive3:

# 3. Verify
rclone lsd gdrive_union:
```

MEGA recovery

```
# 1. Recover MEGA access
# - Go to mega.nz/recovery
# - Use Recovery Key (saved in password manager)
# - Or use recovery email

# 2. Reconfigure rclone
rclone config reconnect mega1:
rclone config reconnect mega2:

# 3. Verify
rclone lsd mega_union:
```

POST-DISASTER CHECKLIST

After every recovery, verify:

```
# 1. Repositories intact
restic -r rclone:gdrive_union:/restic-backup check
restic -r rclone:mega_union:/restic-backup check
```

```
# 2. Recent snapshots exist
restic -r rclone:gdrive_union:/restic-backup snapshots | tail -10

# 3. Critical files recovered
ls -la ~/Desktop/Memories/
ls -la ~/Desktop/Photos/

# 4. Automation reactivated
launchctl list | grep restic

# 5. Passwords saved correctly
security find-generic-password -a "$USER" -s "restic-backup" -w

# 6. Backup test works
~/.local/share/restic-backup/Scripts/backup-desktop.sh
```

KEY LESSONS

1. **Test recovery BEFORE disaster**
2. **3 minimum copies** (local + 2 cloud)
3. **ALSO backup configurations** (rclone.conf, scripts)
4. **Written recovery plan**
5. **Periodic verification** (daily: backup + check)
6. **Passwords saved in 3+ places** (password manager + USB + safe)