

You are here because someone you love has died, and there was no digital plan left behind. That is not unusual -- most people do not leave one. Right now, the most important thing is to take care of yourself and the people around you. The digital world will still be there when you are ready. This section covers only the things that are genuinely time-sensitive, and even among those, very few need to happen today.

Secure the Devices

Locate all devices: phones, tablets, laptops, desktops, smart watches, e-readers

Plug in and charge every device immediately -- a dead battery can mean lost data

Do NOT wipe, reset, or update any device -- updates can trigger re-authentication and lock you out

If any device is unlocked, disable auto-lock right now before it locks itself

If you know the passcode for any device, unlock it and disable auto-lock

If you do not know the passcode, set the device aside safely -- do not guess randomly (some devices erase after 10 failed attempts)

Locate any physical security keys (YubiKey or similar USB/NFC devices) on keychains or near the computer

Write down the make, model, and status (locked/unlocked/powerd on/off) of every device you find

Biometric login (Face ID, fingerprint) will stop working, but the backup PIN or passcode is what you need. Check if the device has a backup PIN set.

Devices located and status:

THIS CAN WAIT

Social media accounts do not need attention in the first few days. Profiles will remain as they are. Closing or memorializing any account can also wait -- doing it prematurely can lock you out of data you may want later.

Secure the Email

Check if email is already accessible through an open browser session on any computer or tablet

If a browser session is open, do NOT sign out -- this access is fragile and may not survive a restart

Check for urgent messages: financial alerts, bills due, pending transactions, legal notices

Watch for password reset emails that might indicate someone else is trying to access accounts

Search the email for 'password' or 'sign in' -- people sometimes email themselves credentials

Do NOT delete any emails -- you will need them for account discovery and estate settlement

If you find email access, change the recovery phone/backup email to your own (if you are the legal executor)

Email access status:

Preserve the Phone and SIM

- Keep the phone charged and powered on -- it may be receiving 2FA verification codes you need
- Do NOT cancel the phone plan yet -- you need the number active for account recovery
- If the phone is unlocked, check for authenticator apps and photograph every entry
- If the phone is unlocked, move the SIM card to a phone you control so you can receive SMS codes
- If the phone uses eSIM (no physical SIM tray), note this -- you will need the carrier's help later
- Keep the phone accessible, not stored away -- you may need it at any moment for verification codes

If the phone number is disconnected or reassigned, you lose the ability to receive SMS verification codes for every account that uses text-based two-factor authentication.

Immediate Financial Triage

CRITICAL WARNING

Determine whether each financial account is jointly owned, solely owned, or has a payable-on-death (POD) beneficiary designation BEFORE contacting any bank. Notifying a bank that an account holder has died can trigger an immediate freeze on sole accounts, locking a surviving spouse out of funds until probate completes. Check ownership first; consult an estate attorney for sole accounts.

- For joint accounts: the surviving owner retains full access -- notify the bank to remove the deceased's name
- For sole accounts: notification will trigger an immediate freeze -- ensure you have alternative funds first
- For POD/TOD accounts: these transfer directly to the named beneficiary outside of probate
- If unsure of account type, consult with an estate attorney before notifying the bank
- Search email for 'receipt,' 'subscription,' 'renewal,' 'payment,' 'invoice' to identify recurring charges
- Identify which autopay items are critical (mortgage, utilities, insurance) versus which to cancel

Financial account ownership and actions:

THIS CAN WAIT

Non-essential subscriptions (streaming services, small recurring charges) do not need to be cancelled in the first few days. A few weeks of charges will not materially affect the estate. Focus only on large charges or accounts draining sole-owner funds.

Smart Home Immediate Actions

- If locked out of smart locks, use physical backup keys
- If unable to control thermostat, look for manual override on the device itself
- If security cameras are recording and you cannot access them, unplug for privacy

If Alexa/Google Home has purchasing enabled, unplug until you can reconfigure

Contact the security monitoring company to transfer or cancel service

Write down which smart home devices exist and their current status

Smart home actions taken:

When someone dies without leaving a list of their accounts, figuring out what exists can feel like searching in the dark. The good news is that digital accounts leave traces everywhere -- in email inboxes, bank statements, browser histories, and the apps on a phone screen. You do not need to find everything at once. Each clue leads to the next, and a partial picture is still valuable.

Email Search Patterns

Once you have access to any email account, use these search terms:

- Search for 'welcome to' or 'thanks for signing up' or 'verify your email'
- Search for 'confirm your account' or 'activate your account'
- Search for 'subscription,' 'receipt,' 'invoice,' 'payment,' 'renewal,' 'billing'
- Search for 'password reset' or 'forgot password' to find previously recovered accounts
- Search for 'two-factor' or 'verification code' to find accounts with 2FA enabled
- Search for 'statement available,' 'account alert,' 'direct deposit' to find financial accounts
- Search platform names one by one: Amazon, Netflix, Spotify, Apple, Google, Facebook, PayPal
- Look in the spam/junk folder -- marketing emails reveal accounts you might otherwise miss
- Check email folders and labels the person created
- Search for 'unsubscribe' to find marketing emails from services with active accounts
- Search for 'order confirmation' or 'shipping' to find e-commerce accounts

THIS CAN WAIT

Building a master account spreadsheet is helpful but not urgent. A notebook, a stack of sticky notes, or a running list in your phone works fine. Organization can come later.

Bank and Credit Card Statement Review

- Gather the most recent 3 to 6 months of bank and credit card statements
- Highlight every recurring charge -- each one represents a subscription or service
- Look for charges from Apple, Google, Amazon, PayPal, and other payment processors
- Check for small verification charges (\$0.01 to \$1.00) indicating recently linked accounts
- Look for annual charges that may not appear every month
- Request a deceased person's credit report from all three bureaus

Credit Bureau Addresses

Equifax: P.O. Box 105139, Atlanta, GA 30348

Experian: P.O. Box 4500, Allen, TX 75013

TransUnion: P.O. Box 2000, Chester, PA 19016

Physical Clue Hunting

- Look for sticky notes near the computer with passwords or account names
- Check notebooks, journals, or index cards for login information
- Check for a physical safe, lockbox, or 'important papers' location
- Look for hardware security keys (small USB devices) near the computer or on their keychain
- Check their wallet for loyalty cards, membership cards, and store credit cards
- Look for printed password manager emergency kits
- Check filing cabinets for printed account statements or financial records
- Check with their attorney, accountant, or financial advisor

Browser History and Saved Passwords

If a browser has saved passwords, this is often the most complete discovery method. A single browser may contain dozens or hundreds of saved credentials.

- Chrome: Settings > Passwords (or <chrome://settings/passwords>)
- Safari: System Settings > Passwords (Mac) or Settings > Passwords (iPhone/iPad)
- Firefox: Settings > Privacy & Security > Saved Logins
- Edge: Settings > Passwords (or <edge://settings/passwords>)
- Check browser bookmarks and history for frequently visited sites
- Try typing common site names in the address bar and see what auto-completes
- Export or photograph all saved passwords before the device locks or is reset

Phone App Inventory

- Photograph every screen of the phone's home screen (each app icon is a potential account)
- Check the App Library (iPhone) or app drawer (Android) for hidden apps
- Check for authenticator apps and photograph every entry
- Check notification center and lock screen for recent app notifications
- On iPhone: Settings > [Name] > Subscriptions for active App Store subscriptions
- On Android: Google Play > Menu > Subscriptions for active Play Store subscriptions
- Look for banking, investment, and payment apps (Venmo, Cash App, Zelle, PayPal)

Master account list or spreadsheet location:

Getting into someone's accounts after they have died is one of the most frustrating parts of this process. Every platform has its own rules, its own required paperwork, and its own timeline. Some are surprisingly cooperative. Others feel needlessly difficult when you are already dealing with so much. This section walks through the major platforms one at a time, so you know what to expect before you start.

THIS CAN WAIT

Non-email account recovery (social media, streaming, shopping) can wait weeks or months unless an account is actively being misused or draining significant funds. Email is the priority. Once you have email access, most other accounts become easier through password resets.

Google (Gmail, Drive, Photos)

Go to Google's deceased user support page: support.google.com/accounts/troubleshooter/6357590

Select what you want: obtain data, request account closure, or report Google Pay funds

Gather: your government-issued photo ID

Gather: the deceased person's death certificate

Gather: proof of your legal authority (executor letters, letters testamentary, or power of attorney)

For data requests: you will also need a U.S. court order specifically naming Google and the data requested

Submit the initial request and wait for Google's review (2 to 6 weeks)

If approved, Google provides template language for the required court order

Work with your attorney to obtain the court order (2 to 4 weeks additional)

Google will never provide the account password or allow you to sign in. Total expected timeline: 1 to 4 months. Practical workaround: check for an open Chrome session and `chrome://settings/passwords` on any unlocked computer.

Apple (iCloud, Photos, Messages)

With Legacy Contact

Go to digital-legacy.apple.com

You need: your Legacy Contact access key AND a certified death certificate

Apple creates a special legacy access account (1 to 2 weeks)

Access lasts up to 3 years before Apple permanently deletes the account

Without Legacy Contact (Court Order Required)

Apple requires a court order naming you as rightful inheritor

Gather: death certificate, court order, your government-issued ID

Submit through Apple Support or at an Apple Store

Processing: several weeks to months

Apple provides: photos, videos, messages (if backed up), notes, files, contacts, calendar, health data. Apple does NOT provide: Keychain passwords, payment info, purchased media (music, movies, apps), or the account password.

Microsoft (Outlook, OneDrive, Xbox)

Contact Microsoft Support and request the Next of Kin process

Gather: certified death certificate

Gather: document proving your legal relationship as a close relative

A court order or subpoena may also be required depending on data sought

If approved, data is delivered on a physical DVD shipped to your address

Important: Outlook.com and OneDrive data may be deleted after 1 year of inactivity. Microsoft accounts expire entirely after 2 years. Submit your request promptly. Timeline: 4 to 8 weeks.

Facebook

Request memorialization at facebook.com/help/contact/305593649477238

Provide proof of death: obituary link, death certificate, or other documentation

To request a data download without a Legacy Contact, you may need a court order

A verified family member can request permanent account deletion

CRITICAL WARNING

Do NOT request memorialization until you have accessed any content you need through an active device session. Once memorialized, all active sessions are terminated and no one can sign in again.

Phone Carrier Number Transfer

Identify the carrier (check the phone, bank statements, or call the number)

Contact the carrier to transfer the number to your account (not cancel it)

Have ready: death certificate, executor documentation, account number or last four of SSN

Verizon (800-922-0204): executor transfer form; 3 business days

AT&T (800-331-0500): Transfer of Billing Responsibility form

T-Mobile (877-746-0909): call customer service; less strict documentation

Password Manager Recovery

Determine which password manager was used (apps on phone/computer, browser extensions)

Check if Emergency Access or a family plan was set up

Look for the master password: sticky notes, notebooks, printed emergency kits

If the app is still signed in on any device, access it immediately before it locks

If no emergency access was configured and you do not have the master password, the vault is permanently inaccessible

Locked Device Strategies

Locked iPhone

Try common personal PINs: birthdate, anniversary, street address numbers

Proceed with extreme caution -- after 10 failed attempts, the phone may erase itself

If locked but SIM is active, incoming 2FA codes may appear on the lock screen

Locked Mac or Windows PC

Mac with FileVault: check if recovery key was escrowed to the Apple ID

Mac without FileVault: boot into Recovery Mode and use Reset Password utility

Windows with BitLocker: check for recovery key at aka.ms/myrecoverykey

Windows without BitLocker: reset password using a Windows installation USB

Account recovery status and ticket numbers:

Every platform has its own policies about what happens to an account when someone dies. Some let you download data. Some let you memorialize the profile. Some will only delete the account entirely. This section is a reference you can come back to as needed -- you do not need to read it all at once.

THIS CAN WAIT

Deciding what to do with social media profiles is not urgent. You do not need to memorialize, delete, or do anything with these accounts right now. Take as much time as you need. There is no wrong timeline.

Platform Quick Reference

Platform	Can Do	Cannot Do	Required Docs
Google	Data export, account closure	Get password, sign in	ID, death cert, court order
Apple	Photos, messages, files, backups	Keychain passwords, purchased media	Legacy key + death cert OR court order
Facebook	Memorialize, download data, delete	Sign in, read messages	Proof of death; court order for data
Instagram	Memorialize or delete	Access data, manage account	Proof of death
X (Twitter)	Request deactivation	Access data, memorialize	Death cert, ID, proof of relation
LinkedIn	Memorial page or closure	Access data, download	Death cert, proof of relation
Microsoft	Email + contacts on DVD	Sign in, transfer ownership	Death cert, proof of relation
TikTok	Request deletion	Memorialize, access data	Death cert, proof of relation
Snapchat	Request deletion	Transfer, recover content	Death cert
Pinterest	Request deactivation	Access boards, transfer	Death cert, proof of relation

Timeline Expectations

Platform	With Legacy Tool	Without Legacy Tool	Court Order Path
Google	N/A (must pre-configure)	1 to 4 months	2 to 4 weeks for order
Apple	1 to 2 weeks	1 to 3 months	2 to 6 weeks for order
Facebook	1 to 4 weeks	1 to 4 weeks	Varies
Microsoft	N/A	4 to 10 weeks	May be required for OneDrive

Platform policies change periodically. If information here does not match what you encounter, check the platform's current help center for their most recent bereavement policy.

You do not have to do this alone, and in many cases, you should not try. Some parts of this process require legal expertise. Some require technical skills. And some just require someone who can sit with you and make phone calls while you take a break. This section helps you identify who can help with what, so you can focus your own energy where it matters most.

When to Hire an Estate Attorney

- The deceased had significant assets (financial accounts, property, investments, businesses)
- Any account is solely owned and you need access to funds for living expenses
- You need a court order to access digital accounts (Google, Apple, Microsoft require this)
- There is no will and you need letters of administration from probate court
- There are disputes among family members about the estate
- The deceased owned cryptocurrency in self-custody (complex legal and tax issues)
- The deceased owned a business, domain names, or revenue-generating online accounts
- Ask specifically whether the attorney has experience with digital estate issues

Many estate attorneys offer a free initial consultation. Bring your master account spreadsheet and a list of what you are locked out of.

Attorney name and contact:

Finding Tech-Savvy Help

- Ask a trusted, tech-savvy friend or family member to help with mechanical tasks
- Be specific: calling carriers, filling out forms, searching email, cancelling subscriptions
- What NOT to share with helpers: master passwords, full financial access, SSNs, seed phrases
- If you delegate device access, stay present or set clear boundaries
- Consider a professional digital estate organizer if the volume is overwhelming

Cryptocurrency Recovery

CRITICAL WARNING

Be extremely cautious of crypto recovery scams. Never share seed phrases or private keys with anyone who contacts you unsolicited. Legitimate recovery services do not contact you first -- you contact them. Never send cryptocurrency to 'verify' or 'unlock' a wallet.

- Only consider professional recovery if you have partial information (partial seed phrase, possible passwords)
- Legitimate firms: Wallet Recovery Services, Brute Brothers, KeychainX -- research each before engaging
- Legitimate firms typically charge 15% to 30% of recovered funds (success-based fee)
- If the seed phrase is completely unknown and no partial info exists, recovery is not possible

Government Agencies to Notify

- Social Security Administration: call 1-800-772-1213 to report the death
- IRS: send death certificate copy to flag the SSN against fraudulent tax filings
- DMV: cancel the driver's license to prevent identity theft
- USPS: notify to forward or hold mail; cancel any Informed Delivery account
- Credit bureaus: send certified death certificate copies to all three (see B-06 for addresses)
- State tax authority: notify as required by your state
- Veterans Affairs (if applicable): call 1-800-827-1000

THIS CAN WAIT

Finding a grief counselor can wait -- but not forever. If you are managing day to day, professional support can wait until you are ready. But if you are struggling to function, reaching out sooner is an act of self-care, not weakness.

Grief and Support Resources

- The Dougy Center:** dougy.org -- grief support for children and families
- GriefShare:** griefshare.org -- local and online support groups
- Nat'l Alliance for Grieving Children:** childrengrieve.org
- 988 Suicide and Crisis Lifeline:** call or text 988 for immediate support
- GYST:** getyourshittogether.org -- Chanel Reynolds' original resource

Money is often the most stressful part of navigating a loss, and the digital world can make it harder. Subscriptions charge silently. Autopay keeps running. Bank accounts may freeze the moment you notify the institution. Before you take any financial action, read the warning below.

Joint vs. Sole Account Ownership

CRITICAL WARNING

Check the account ownership type for EVERY financial account BEFORE notifying the institution of the death. For joint accounts, the surviving owner retains full access. For sole accounts, notification triggers an immediate freeze -- the surviving family may lose access to funds until probate completes, which can take months. If unsure of account type, consult an estate attorney before calling the bank.

For each bank account, determine: joint (both names), sole (deceased only), or POD/TOD beneficiary

For joint accounts: notify the bank to remove the deceased and update ownership

For sole accounts: ensure you have alternative funds for living expenses before notifying

For POD/TOD accounts: these pass directly to the named beneficiary outside probate

Check credit card accounts the same way -- joint holders are not liable for sole-cardholder debts in most states

Check investment and brokerage accounts for TOD beneficiary designations

For retirement accounts (401k, IRA): check with the plan administrator for named beneficiaries

Account ownership determinations:

Subscription Cancellation Triage

Search email for 'subscription,' 'receipt,' 'renewal,' 'billing,' 'payment,' 'membership'

Check app store subscriptions (iPhone: Settings > [Name] > Subscriptions; Android: Google Play > Subscriptions)

Check PayPal, Venmo, and other payment platforms for recurring payment agreements

Prioritize cancellations: highest monthly charges first, then services no longer needed

Keep services that others in the household still use (family streaming plans, internet, utilities)

Do NOT cancel domain registrations without understanding if they are needed for business or email

Address Buy Now Pay Later balances (Affirm, Klarna, Afterpay) -- these are debts for the estate attorney

Watch for annual renewals that may not appear for months -- set calendar reminders

Subscriptions cancelled (service, date, confirmation):

THIS CAN WAIT

Low-cost subscriptions (streaming services, small recurring charges) do not need to be cancelled right away. A few months of charges will not materially affect the estate. Focus on large recurring charges first.

Identity Theft Protection

Deceased persons are targets for identity theft. Thieves monitor obituaries and public death records. An estimated 2.5 million deceased individuals are victims of identity fraud annually.

Notify SSA of the death (1-800-772-1213)

Send certified death certificate copies to all three credit bureaus; request 'deceased' flag and freeze

Send death certificate copy to the IRS to flag the SSN

Cancel the driver's license with the DMV

Notify USPS to forward or hold mail -- identity thieves monitor mailboxes of the deceased

If an obituary is published, omit full birthdate, maiden name, and address

Be wary of bereavement scams from people using obituary details

File an identity theft report at identitytheft.gov if you discover fraudulent activity

Credit Bureau Addresses

Equifax: P.O. Box 105139, Atlanta, GA 30348

Experian: P.O. Box 4500, Allen, TX 75013

TransUnion: P.O. Box 2000, Chester, PA 19016

Ongoing Financial Monitoring

Monitor credit reports monthly for at least the first year

Continue monitoring quarterly for at least one additional year (24 months total)

Watch for new accounts opened in the deceased's name

Watch for annual subscription renewals that surface months later

Google the deceased's name periodically to catch unauthorized identity use

Remove the deceased from data broker sites (or use a service like DeleteMe)

Retain copies of death certificate, letters testamentary, and all correspondence

Financial monitoring notes:

At some point during this process, you will encounter something that stops you in your tracks. A text message that reads like they are still here. A photo you have never seen before. An AI-generated 'memory' notification from a platform that does not know they have died. The practical work of managing someone's digital life is intertwined with the emotional reality of loss in ways that nothing else quite matches. This section is not a checklist. It is permission to pause.

THIS CAN WAIT

Everything in this section can wait. There is no item here that is time-sensitive. Every part of the emotional work of processing someone's digital life can happen on your timeline. Months from now. Years from now. Or never, if that is what feels right.

Taking Care of Yourself

- Set a timer when working through digital accounts -- commit to stopping after a defined period
- Take breaks between emotionally charged tasks and mechanical tasks
- Delegate mechanical tasks to a trusted helper: calling carriers, cancelling services, filling out forms
- Keep tasks that require personal judgment for yourself: what to memorialize, delete, save, or read
- Do not force yourself to look through photos, messages, or personal content until you are ready
- Keep a notebook nearby to write down thoughts or memories that surface
- Accept that this process will take months, not days -- give yourself permission to set it aside

Platform Notification Management

Platforms like Google Photos, Apple Photos, and Facebook generate automated 'On This Day' or 'memory' notifications that can be devastating when they feature someone who has died. Turning these off is one area where acting sooner may be worth the effort.

- Facebook: Settings > Memories > turn off memory notifications
- Google Photos: Settings > Memories > hide specific people or time periods
- Apple Photos: For You tab > long press a memory > Delete Memory (or hide specific people)
- Unsubscribe from marketing emails sent to the deceased's accounts
- Turn off app notifications on the deceased's devices to stop constant pinging
- If the deceased's email forwards to yours, filter those messages to a separate folder

Deciding What to Do With Accounts

For each account or digital artifact, consider four options:

- Memorialize:** Keep the account visible as a tribute. The profile is marked as belonging to someone who has died. Choose this when the online presence is meaningful.
- Delete:** Permanently remove the account. Choose this for accounts with no sentimental value or that pose identity theft risk.
- Archive:** Download all content and then close the account. Choose this when you want to preserve memories privately without maintaining a public presence.

Leave alone: Do nothing for now. This is a valid choice. Some accounts can remain dormant while you focus on higher-priority items. You do not owe anyone an explanation for your choices.

Exceptions to be aware of: Microsoft accounts expire after 2 years of inactivity. Apple Legacy Contact access expires after 3 years.

When You Find Unexpected Content

People are complex. Everyone has parts of their life that are private. Discovering something you did not expect does not change who the person was to you.

You are not obligated to read everything -- you can close a conversation or app and come back later

If you find content involving potential harm to others, consult with an attorney

If you find evidence of unknown financial obligations, document them for the estate attorney

Talk to a counselor or trusted person if unexpected discoveries are weighing on you

Do not share the deceased's private content publicly without careful consideration

Grief Support Resources

The Dougy Center: dougy.org -- grief support for children, teens, and families

GriefShare: griefshare.org -- support groups (in-person and online)

Nat'l Alliance for Grieving Children: childrengrieve.org

988 Suicide and Crisis Lifeline: call or text 988

GYST: getyourshitttogether.org -- Chanel Reynolds' original resource

Identity Theft Resource Center: idtheftcenter.org -- if identity theft adds to your stress

The digital estate work can wait. You cannot pour from an empty cup. If you need to stop and take care of yourself, stop and take care of yourself.