Account Inventory Checklist

Before you can plan for anything, you need to know what exists. Most people vastly underestimate the size of their digital footprint. The average person has well over 100 online accounts. For every account, record the service name, your username/email, and what the account is used for. **Do not put passwords in this list** -- that is handled separately.

Email Accounts

- [ ] Primary personal email (Gmail, Outlook, Yahoo, ProtonMail, etc.)
- [ ] Secondary/backup email accounts
- [ ] Work or professional email accounts
- [ ] Legacy email accounts you still have but rarely use
- [ ] Email aliases or forwarding addresses

Additional Email Accounts accounts / notes:

Financial & Banking

- [ ] Bank accounts (checking, savings, money market)
- [ ] Credit card accounts and portals
- [ ] Investment and brokerage accounts
- [ ] Retirement accounts (401k, IRA portals)
- [ ] Cryptocurrency wallets, exchanges, and DeFi accounts
- [ ] Payment platforms (PayPal, Venmo, Zelle, Cash App, Apple Pay, Google Pay)
- [ ] Tax preparation services (TurboTax, H&R Block, etc.)

- [ ] Peer-to-peer lending or crowdfunding accounts
- [ ] Buy Now Pay Later accounts (Affirm, Klarna, Afterpay)

Additional Financial & Banking accounts / notes:

Social Media & Communication

- [ ] Facebook / Meta
- [ ] Instagram
- [ ] X (Twitter)
- [ ] LinkedIn
- [ ] TikTok
- [ ] Snapchat
- [ ] Reddit
- [ ] YouTube (if separate from Google)
- [ ] Threads, Bluesky, Mastodon, or other newer platforms
- [ ] Discord servers (especially if you own/admin any)
- [ ] WhatsApp, Signal, Telegram
- [ ] Dating apps (if applicable)

- [ ] Forums or community boards you participate in

Additional Social Media & Communication accounts / notes:

Cloud Storage & Photos

- [ ] Google Drive / Google Photos
- [ ] iCloud / Apple Photos
- [ ] Dropbox
- [ ] OneDrive
- [ ] Box
- [ ] Amazon Photos
- [ ] Other cloud backup services (Backblaze, Carbonite, etc.)
- [ ] Photo printing/book services with stored photos (Shutterfly, Mixbook, etc.)

Additional Cloud Storage & Photos accounts / notes:

Subscriptions & Recurring Services

- [ ] Streaming video (Netflix, Hulu, Disney+, Max, Paramount+, etc.)
- [ ] Streaming music (Spotify, Apple Music, Amazon Music, Tidal, etc.)

- [ ] News and media subscriptions (NYT, WSJ, Substack, etc.)
- [ ] Software subscriptions (Adobe, Microsoft 365, etc.)
- [ ] Gaming subscriptions (PlayStation Plus, Xbox Game Pass, Steam, etc.)
- [ ] Meal kit or grocery delivery (HelloFresh, Instacart, etc.)
- [ ] Fitness and health apps (Peloton, gym memberships, meditation apps)
- [ ] AI services (ChatGPT Plus, Claude Pro, Midjourney, etc.)
- [ ] VPN services
- [ ] Domain registrations and website hosting
- [ ] Cloud computing services (AWS, Azure, Google Cloud)

Additional Subscriptions & Recurring Services accounts / notes:

Shopping & E-Commerce

- [ ] Amazon
- [ ] eBay
- [ ] Etsy
- [ ] Walmart, Target, and other retail accounts
- [ ] Grocery delivery accounts
- [ ] Any accounts with stored payment methods or shipping addresses

Additional Shopping & E-Commerce accounts / notes:

Healthcare & Insurance Portals

- [ ] Health insurance portal
- [ ] Medicare/Medicaid portals
- [ ] MyChart or other patient portals
- [ ] Pharmacy accounts (CVS, Walgreens, mail-order)
- [ ] Dental, vision, and specialist portals
- [ ] Life insurance online portals
- [ ] FSA/HSA account portals
- [ ] Mental health app accounts (BetterHelp, Talkspace, etc.)

Additional Healthcare & Insurance Portals accounts / notes:

Government & Official Accounts

- [ ] Social Security Administration (ssa.gov / my Social Security)
- [ ] IRS account (irs.gov)
- [ ] State tax portal

- [ ] DMV / driver's license renewal portal
- [ ] Veterans Affairs (va.gov) if applicable
- [ ] USPS Informed Delivery
- [ ] Voter registration portal
- [ ] TSA PreCheck / Global Entry / CLEAR
- [ ] Passport renewal portal
- [ ] Login.gov and/or ID.me accounts

Additional Government & Official Accounts accounts / notes:

Smart Home, IoT & Connected Devices

- [ ] Smart home hub accounts (Google Home, Alexa, HomeKit, SmartThings)
- [ ] Smart thermostat (Nest, Ecobee)
- [ ] Security cameras and doorbells (Ring, Nest, Wyze, Arlo, SimpliSafe)
- [ ] Smart locks and garage door openers
- [ ] Robot vacuums (iRobot, Roborock)
- [ ] Smart lighting (Hue, LIFX)
- [ ] Vehicle accounts and connected car apps (Tesla, FordPass, OnStar, etc.)

- [ ] Pet tech (smart feeders, GPS trackers, vet portals)
- [ ] Wearables (Fitbit, Garmin, Whoop, Apple Watch health data)

Additional Smart Home, IoT & Connected Devices accounts / notes:

Professional & Business

- [ ] Professional licenses with online portals
- [ ] Business accounts you own or administer
- [ ] Freelance platform accounts (Upwork, Fiverr, etc.)
- [ ] Domain names you own (and which registrar)
- [ ] Websites or blogs you maintain
- [ ] Professional association memberships
- [ ] CRM or business tool logins
- [ ] Intellectual property registrations

Additional Professional & Business accounts / notes:

Loyalty Programs & Rewards

- [ ] Airline miles accounts

- [ ] Hotel loyalty programs
- [ ] Credit card rewards portals
- [ ] Retail loyalty programs with stored value
- [ ] Cashback programs (Rakuten, Ibotta, etc.)

Additional Loyalty Programs & Rewards accounts / notes:

Digital Content & Purchases

- [ ] E-books (Kindle, Nook, Kobo)
- [ ] Digital music purchases (iTunes, Amazon)
- [ ] Digital movie/TV purchases
- [ ] Video game libraries (Steam, PlayStation, Xbox, Nintendo, Epic, GOG)
- [ ] App purchases (iOS App Store, Google Play)
- [ ] NFTs or digital collectibles (if applicable)

Additional Digital Content & Purchases accounts / notes:

Important: *Most digital content (e-books, music, movies, apps) is licensed, not owned. This means it generally cannot be transferred or inherited. Your family may lose access to your Kindle library, iTunes purchases, etc.*

Password & Access Plan

This is the single most impactful thing you can do for your survivors. Without access credentials, your loved ones face an uphill battle with every single account -- often requiring death certificates, court orders, and weeks of waiting per account.

2.1 -- Password Manager Setup

- [ ] Choose and set up a password manager (1Password, Bitwarden, Dashlane, LastPass, Keeper)
- [ ] Migrate existing passwords from browsers, sticky notes, and memory into the password manager
- [ ] Ensure every account has a unique, strong password
- [ ] Set up the password manager's emergency access or family sharing feature

Emergency Access Features by Manager

- [ ] 1Password: Family/Teams account; share a vault; store Emergency Kit in physical safe
- [ ] Bitwarden: Emergency Access feature with trusted contact and waiting period
- [ ] Dashlane: Emergency Contact feature
- [ ] LastPass: Emergency Access feature with trusted contact and waiting period
- [ ] Keeper: Emergency Access (KeeperChat) feature

Password manager chosen and emergency access details:

2.2 -- Two-Factor Authentication (2FA) Planning

2FA protects your accounts while you are alive, but it can lock everyone out after you die if not planned for.

- [ ] Document which accounts have 2FA enabled
- [ ] Store 2FA backup/recovery codes in password manager AND physical location
- [ ] Document which authenticator app you use and what device it is on
- [ ] Consider Authy (multi-device sync) instead of Google Authenticator (device-bound)
- [ ] If you use a hardware security key (YubiKey, Titan), document its physical location and register backups
- [ ] Store your phone's passcode/PIN securely
- [ ] Document your phone carrier's account PIN/password (needed for SIM transfers)

2FA details and recovery code storage locations:

2.3 -- Device Access

- [ ] Document passcode/PIN/password for every device: phones, tablets, laptops, desktops
- [ ] Document biometric backup methods (backup PINs for Face ID / fingerprint)
- [ ] Document Apple ID or Google account password tied to each device
- [ ] Note any encrypted drives or volumes and their decryption passwords
- [ ] Record location of recovery keys for disk encryption (FileVault, BitLocker)
- [ ] If you have a NAS or home server, document its admin credentials

Device access notes:

2.4 -- Physical Storage of Access Information

- [ ] Store master password and emergency kit in fireproof safe, safe deposit box, or with attorney
- [ ] Consider splitting sensitive info (master password in one location, emergency kit in another)
- [ ] Let your executor/trusted person know WHERE this information is stored
- [ ] Review and update this information at least annually

Storage locations and trusted persons:

Platform Legacy Settings

Many major platforms now offer built-in tools to manage what happens to your account. Setting these up takes minutes and saves your survivors enormous headaches.

Google (Gmail, Drive, Photos, YouTube)

- [ ] Set up Google Inactive Account Manager at myaccount.google.com/inactive
  - [ ] Choose inactivity timeout period (3, 6, 12, or 18 months)
  - [ ] Add up to 10 trusted contacts to notify and/or share data with
  - [ ] Choose which data types each contact receives
  - [ ] Decide whether to auto-delete the account after contacts are notified

If you have a YouTube channel with subscribers or revenue, this is especially important.

Google legacy contacts and settings:

Apple (iCloud, Photos, Messages)

- [ ] Set up Apple Legacy Contacts: Settings > [Your Name] > Sign-In & Security > Legacy Contact (iOS 15.2+)
  - [ ] Add up to 5 Legacy Contacts
  - [ ] Share generated access key with each contact (print, AirDrop, or Messages)

Legacy Contacts cannot access Keychain passwords, payment info, or licensed media. Apple will permanently delete the account 3 years after Legacy Contact access is granted.

Apple legacy contacts:

Facebook / Meta

- [ ] Set up Legacy Contact: Settings > Accounts Center > Personal Details > Account Ownership > Memorialization
  - [ ] Choose whether Legacy Contact can download a copy of your data
  - [ ] Alternatively, choose to have account permanently deleted after death

Legacy Contacts can pin a tribute post, change profile/cover photo, accept friend requests -- but cannot read messages, remove content, or log in as you.

Instagram

No legacy contact feature. Account can only be memorialized or deleted by a verified family member.

- [ ] Download your data periodically (Settings > Your Activity > Download Your Information)

X (Twitter)

No legacy contact or memorialization feature. Verified family member can request deactivation.

LinkedIn

No legacy contact feature. Verified family member can request memorial page or closure.

- [ ] Export your connections and data periodically

Microsoft (Outlook, OneDrive, Xbox)

Microsoft's Next of Kin process allows limited data access with a court order, death certificate, and proof of relationship. Accounts auto-close after 2 years of inactivity. Among the more restrictive policies -- plan accordingly.

Other Platforms

- [ ] Check each platform you use for legacy/inactive account settings
- [ ] For platforms with no legacy tools, ensure credentials are in your password manager

Other platform legacy settings configured:

3.2 -- Email-Specific Considerations

Your primary email is often the skeleton key to your entire digital life -- it is the recovery address for almost every other account. Securing email access for your executor is the single highest-priority digital planning task.

- [ ] Ensure your executor can access your primary email
- [ ] Consider setting up forwarding or shared access with a trusted person
- [ ] Document which email is the recovery address for your major accounts

Quick Reference: Platform Death/Legacy Policies

Platform	Legacy?	Feature Name	Key Limitation
Google	Yes	Inactive Account Manager	Must be set up while alive
Apple	Yes	Legacy Contact	Access key required; deleted after 3 yrs

Facebook	Yes	Legacy Contact	Cannot read messages or log in
Instagram	No	N/A	Memorialize or delete only
X (Twitter)	No	N/A	Request deactivation with docs
LinkedIn	No	N/A	Request memorial or closure
Microsoft	Limited	Next of Kin process	Requires court order
TikTok	No	N/A	No formal memorialization
Snapchat	No	N/A	No account transfer
Pinterest	No	N/A	Request deactivation

Digital Executor Designation

4.1 -- Choosing Your Digital Executor

Your digital executor may or may not be the same person as the executor of your will. Choose someone who is comfortable with technology, trustworthy with sensitive information, and ideally tech-savvy enough to navigate online account recovery processes.

- [ ] Choose a digital executor (and a backup)
- [ ] Have a conversation with them about the role and what it involves
- [ ] Show them where your password manager emergency information is stored
- [ ] Let them know about this guide

Primary digital executor:

Backup digital executor:

Date of conversation with executor(s):

4.2 -- Legal Authorization

RUFADAA (Revised Uniform Fiduciary Access to Digital Assets Act), adopted in 48 U.S. states, provides a framework, but explicit consent in your estate documents is strongest.

- [ ] Include digital assets in your will or trust
- [ ] Specifically authorize your executor to access your digital accounts
- [ ] Consider including language authorizing bypass of 2FA using backup codes
- [ ] Ask your estate planning attorney about a separate digital estate plan document
- [ ] If you hold cryptocurrency, include a specific crypto clause in estate documents

Attorney name and contact:

Legal authorization status and notes:

5.1 -- Cryptocurrency & Digital Financial Assets

Crypto is fundamentally different from bank accounts. There is no customer service number. No one can reset your password. If your private keys or seed phrases are lost, the assets are gone permanently.

- [ ] Document all cryptocurrency holdings (coins/tokens, amounts, wallets, exchanges)
- [ ] Store seed phrases / recovery phrases in a physical, secure location
- [ ] NEVER store seed phrases digitally in a way that could be hacked
- [ ] Consider a hardware wallet (Ledger, Trezor) with device and PIN stored securely
- [ ] Consider multi-signature wallets with a co-signer who is your executor
- [ ] Write plain-language instructions for a non-crypto-savvy person
- [ ] Document which exchanges hold funds and how to access them

Crypto holdings summary and access instructions location:

5.2 -- Businesses, Domains & Online Revenue

- [ ] Document all domains you own and their registrars
- [ ] Ensure domain auto-renewal is on to prevent expiration during estate settlement
- [ ] Document any websites or blogs and their hosting providers
- [ ] Transfer admin access for business social media pages to at least one other person
- [ ] Document any online revenue streams (YouTube, affiliate, Patreon, Substack, etc.)
- [ ] For online businesses, document the tech stack, hosting, and critical vendor relationships
- [ ] If you admin Discord servers, Slack workspaces, or communities, designate co-admins

Domain and business account details:

5.3 -- Smart Home & Connected Devices

When someone dies, their smart home can become an obstacle course for survivors -- locks they can't open, thermostats they can't control, security cameras they can't access or disable.

- [ ] Document the primary account holder for each smart home system
- [ ] Ensure at least one other household member has admin/owner access
- [ ] Document Wi-Fi network name and password

- [ ] Document router admin login
- [ ] List all connected devices and what account controls each one
- [ ] Smart locks: ensure someone else has the master code or physical backup key
- [ ] Security systems: ensure someone else can arm/disarm; know the monitoring company's process
- [ ] Connected vehicles: document how to transfer ownership of connected car accounts
- [ ] Smart speakers/assistants: note voice purchasing settings, calendar info, personal data

Smart home details and secondary account holders:

5.4 -- Photos, Memories & Sentimental Digital Assets

- [ ] Identify where your photos and videos are stored (phone, cloud, external drives)
- [ ] Create at least one consolidated backup of irreplaceable photos on a physical drive
- [ ] Store that drive in a known, safe location and tell someone where it is
- [ ] Consider printing a physical photo book of the most important photos
- [ ] Document any personal writing, journals, or creative work and your wishes for them
- [ ] Note any voicemails, voice messages, or audio recordings you'd want preserved

Photo/media storage locations:

5.5 -- Email and Message Archives

- [ ] Consider using Google Takeout, Apple data export, etc. to download email archives
- [ ] Document your wishes: should your executor read, delete, or preserve your emails?
- [ ] Note any important ongoing email threads your executor may need

Email archive wishes and important threads:

5.6 -- Privacy and Selective Disclosure

This estate plan is a tool for you. It exists to help the people you love navigate your digital life if something happens to you. But it does not have to include everything.

Specific Digital Scenarios

You may have accounts, memberships, or communities that are deeply personal -- things that are part of who you are but that you have chosen not to share with everyone in your life. Gender identity or LGBTQ+ community spaces. Health support groups. Adult content accounts. Personal journals or creative work. Religious or spiritual communities. Political activism. Therapy or mental health platforms. Anonymous accounts where you explored ideas you were not ready to ask about out loud.

These are legitimate parts of your life, and you get to decide whether they are included in your estate plan. There is no obligation to disclose every account. A complete inventory is useful for practical purposes -- it helps your executor find financial accounts, cancel subscriptions, and protect against identity theft. But an estate plan is not a confession, and your executor does not need a map to every corner of your inner life.

If you choose to exclude certain accounts, consider the practical implications. An excluded account with a stored payment method will continue to charge until the payment method expires or is closed. An excluded social media account will remain active indefinitely unless the platform's inactivity policy eventually removes it. If you would prefer that specific accounts be deleted after your death without anyone seeing the contents, some password managers allow you to create a separate vault with instructions to delete without reviewing. This requires a high degree of trust in the designated person, but it is an option.

- [ ] Review your account inventory and decide which accounts to include or exclude
- [ ] For excluded accounts: accept that they will remain active or charge until inactivity policies apply
- [ ] Consider a separate, sealed vault or envelope with 'delete without reading' instructions
- [ ] If using a password manager, consider a separate vault for accounts to be deleted unreviewed
- [ ] Your digital life is yours. Your plan should reflect the boundaries you have set while living.

Privacy decisions and notes:

Identity Theft Protection

An estimated 2.5 million deceased individuals are victims of identity fraud annually. The period immediately after death is especially vulnerable because there is a gap between the death and when government agencies and financial institutions are notified.

6.1 -- Pre-Planning to Reduce Risk

- [ ] Minimize personal information in any future obituary (avoid full birthdate, maiden name, address)
- [ ] Set up credit monitoring or freeze your credit proactively
- [ ] Shred physical documents with sensitive information
- [ ] Be aware that genealogy sites, voter databases, and social media provide info thieves use
- [ ] Consider opting out of data broker sites (services like DeleteMe can help)

Credit freeze status and monitoring service:

6.2 -- Instructions for Your Executor

Leave a note for your executor with these steps so they know what to do quickly:

Critical warning about financial accounts: *Before notifying any bank or financial institution of a death, first determine whether the surviving spouse or partner is a joint account holder. Notifying a bank that an account holder has died can trigger an immediate freeze on the account. If the surviving spouse is not listed on the account, they may lose access to funds until probate is completed, which can take months. Consult an estate attorney before contacting financial institutions about solely-held accounts.*

- [ ] Notify Social Security Administration (1-800-772-1213) as soon as possible
- [ ] Send death certificate copies to all three credit bureaus; request 'deceased' alert and freeze
- [ ] Notify the IRS (to prevent fraudulent tax returns)
- [ ] Cancel the deceased's driver's license with the DMV
- [ ] Determine joint vs. sole account status for every financial account BEFORE notifying the institution
- [ ] For joint accounts: notify the bank to remove the deceased and update account ownership
- [ ] For sole accounts: consult an estate attorney before contacting the institution
- [ ] Monitor credit reports for at least 12 months for new activity
- [ ] Forward or stop physical mail (thieves monitor mailboxes of the deceased)
- [ ] Be cautious of 'bereavement scams' from people using obituary details

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

Identity protection notes:

Immediate Priorities

If you are reading this section, you may be in the middle of one of the hardest experiences of your life. Not everything needs to happen at once. Prioritize based on urgency -- security and financial accounts first, sentimental and social media accounts later.

7.1 -- Secure the Devices

- [ ] Locate all devices: phones, tablets, laptops, desktops, smart watches
- [ ] Do NOT wipe, reset, or update any device. Keep them charged and powered on
- [ ] If you know the passcode, unlock and disable auto-lock temporarily
- [ ] If you don't know the passcode, set the device aside safely for later
- [ ] Check if the phone has biometric login -- the backup PIN is what you need
- [ ] Plug in and charge all devices to prevent data loss from dead batteries
- [ ] Locate any physical security keys (YubiKey, Titan) and keep them safe

Devices located and status:

7.2 -- Secure the Email

- [ ] Access the deceased's primary email as soon as possible
- [ ] Check for urgent messages (financial alerts, bills due, pending transactions)
- [ ] Watch for password reset emails indicating someone else is trying to access accounts
- [ ] Do NOT delete any emails -- you may need them for estate settlement

Email access status:

7.3 -- Stop the Financial Bleeding

Important: *Do NOT notify banks or financial institutions of the death until you know whether each account is joint or solely held. Notifying a bank can freeze the account immediately, locking a surviving spouse out of funds until probate completes. Check account ownership first; consult an estate attorney for sole accounts.*

- [ ] Search email for 'receipt,' 'subscription,' 'renewal,' 'payment,' 'invoice'
- [ ] Review bank and credit card statements for recurring charges
- [ ] Cancel or pause subscriptions actively draining funds
- [ ] Check joint vs. sole ownership on every financial account before contacting the institution
- [ ] For joint accounts: contact the bank to update account ownership
- [ ] For sole accounts: consult estate attorney before notifying the bank
- [ ] Determine which autopay bills are critical (mortgage, utilities, insurance) vs. cancel

Recurring charges found and actions taken:

7.4 -- Smart Home Immediate Actions

If you live in the home and cannot control smart devices:

- [ ] 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 can't access them, unplug for now
- [ ] If Alexa/Google Home has purchasing settings, unplug until you can reconfigure
- [ ] Contact the security monitoring company to transfer or cancel service

Smart home actions taken:

Ongoing Actions

8.1 -- Protect Against Identity Theft (First 1-4 Weeks)

- [ ] Notify Social Security Administration (1-800-772-1213)
- [ ] Send certified death certificate copies to Equifax, Experian, TransUnion
- [ ] Request each bureau flag the file as 'deceased' and freeze credit
- [ ] Send death certificate copy to the IRS to flag the SSN
- [ ] Cancel driver's license with the DMV
- [ ] Monitor deceased's credit reports monthly for at least one year
- [ ] Notify USPS to forward or hold mail
- [ ] Be wary of phishing emails, scam calls, and bereavement scams

8.2 -- Account-by-Account Review (First 1-4 Weeks)

- [ ] Create a master spreadsheet of discovered accounts (name, status, action, date)
- [ ] Prioritize: financial > email > cloud storage > social media > everything else
- [ ] For each account: transfer ownership, memorialize, close/delete, or leave for now
- [ ] Keep records of every call, email, and ticket number
- [ ] Request a deceased person's credit report to discover unknown financial accounts

Account tracking spreadsheet location:

8.3 -- Social Media Decisions (First 1-4 Weeks)

There is no rush on these. Take your time.

- [ ] Decide whether to memorialize, delete, or leave each social media account as-is
- [ ] If memorializing Facebook: use Memorialization Request form or contact Legacy Contact
- [ ] If deleting: gather content you want to preserve FIRST
- [ ] Consider downloading a full data archive from each platform before making changes
- [ ] If accounts are public, consider restricting access to prevent bots/scammers
- [ ] Transfer admin rights for groups, pages, Discord servers, or communities

8.4 -- Subscription Cancellation (First 1-4 Weeks)

- [ ] Search email for all subscription-related emails
- [ ] Check app stores (iOS, Google Play) for active subscriptions

Ongoing Actions

- [ ] Check password manager for accounts with payment methods
- [ ] Cancel streaming, SaaS, and membership subscriptions
- [ ] Contact domain registrars if deceased owned domains
- [ ] Cancel or transfer utility accounts tied to online portals
- [ ] Address any Buy Now Pay Later balances

Subscriptions cancelled (service, date, confirmation):

9.1 -- Digital Asset Settlement (1-6 Months)

- [ ] Work with estate attorney on accounts requiring legal documentation
- [ ] Gather and file paperwork (death certificates, letters testamentary, court orders)
- [ ] Transfer ownership of domains, websites, or online businesses
- [ ] Address cryptocurrency holdings (consult crypto-knowledgeable advisor before moving funds)
- [ ] Determine value of digital assets for the estate
- [ ] File final tax returns noting digital income sources

9.2 -- Data Preservation (1-6 Months)

- [ ] Download and archive photos, videos, and documents from all cloud services
- [ ] Export email archives if desired
- [ ] Save voicemails, voice messages, or audio recordings
- [ ] Back up phone data BEFORE the phone plan is cancelled or device wiped
- [ ] Create consolidated memorial archive on physical drive and/or shared cloud folder
- [ ] Consider creating a printed photo book or physical memorial artifact

9.3 -- Online Presence Cleanup (1-6 Months)

- [ ] Review and update/remove online profiles in search results
- [ ] Remove deceased from data broker sites (or use DeleteMe)
- [ ] Cancel USPS Informed Delivery account
- [ ] Close or remove listings on professional directories
- [ ] Decide on personal website/blog: maintain as memorial, archive, or take down
- [ ] Google the deceased's name periodically to catch unauthorized identity use

10 -- Long-Term Vigilance

- [ ] Continue monitoring credit reports for at least 2 years
- [ ] Watch for annual subscription renewals that appear months later
- [ ] Keep record of all accounts closed, transferred, or memorialized
- [ ] Maintain physical backup of preserved digital memories in safe location
- [ ] Be aware some platforms auto-delete accounts after legacy access period

Long-term monitoring notes: