Your Digital Legacy: A Guide to Tying Up Loose Ends

Why This Matters

We often spend a lot of time organizing our physical affairs—our wills, our homes, and our finances. But in today's world, much of our life exists in places that are invisible: inside our phones, on the "cloud," and in our email inboxes.

When someone passes away, their digital life doesn't automatically shut down. Without your help now, your loved ones may face a difficult struggle later. They might be locked out of family photos, unable to stop monthly subscription charges, or unsure how to handle your social media profiles - even utilities are app-based mobile first these days. Technology companies have strict privacy laws that often make it impossible for family members to access these accounts after the fact.

By taking a little time to organize these details, you are offering a final, profound gift to the people you care about: the gift of clarity and peace of mind.

This guide is designed to help you organize your digital life in stages. Take your time. You can print this guide and check off each item when you are comfortable with it. You don't need to do it all at once.

Overview Checklist:

Phase 0: Protecting Yourself Now is Critical

While preparing this information is an act of love, it creates a "Skeleton Key" to your entire life. At a time when you may feel vulnerable or tired, it is vital to protect yourself from exploitation, coercion, or theft—even from those close to you.

- [ ] **The "Sealed Envelope" Strategy:** You do **not** have to give anyone your passwords today. The safest method is to write the information down, place it in a sealed envelope, sign your name across the flap (so it cannot be opened without you knowing), and store it in a safe place or with your solicitor. Instruct your trusted person that this is only to be opened after you pass.
- [ ] **Beware of Pressure:** If a family member, caregiver, or "helper" is pressuring you to give them your PINs, banking passwords, or device unlock codes "for your own good," **trust your instincts**. You have the right to privacy until the very end. If you feel unsafe or coerced, speak to a lawyer, doctor, or a neutral support agency immediately.
- [ ] **Avoid "Tech Support" Scams:** Scammers often target older adults or those who are ill. Be very suspicious of unsolicited calls or emails offering to "secure your digital assets" or "fix your computer." Only work with established professionals or family members you initiated contact with.

Phase 1: The "Master Keys" & Access

If you only do one section of this list, make it this one. It is easy to rely on "muscle memory" for these tasks, but your loved ones will need written clarity to gain access.

> ⚠️ **Important Safety Note:** Please **do not** write passwords or PIN codes in your formal Last Will and Testament. Wills often become public records after probate, meaning your passwords could become public knowledge. Instead, write this information in a separate document or notebook, store it in a secure place (like a fireproof box or safe), and simply tell your trusted person where to find it.

- [ ] **The Biometric Trap (Face & Fingerprints):** We get used to unlocking our phones with a glance or a fingerprint. However, these features will not work for your family later, and they are not a reliable way to pass on access. **You must write down the actual passcode or PIN** that acts as the backup to your face or fingerprint. Without this code, the device is essentially a brick.
- [ ] **The "Don't Cancel" Warning (Vital):** Please leave a specific note for your family instructing them **NOT** to cancel your mobile phone number immediately. Most accounts (Bank, Email, Social Media) will send a "verification code" to that number when your family tries to log in. Even if you don't typically use SMS codes, systems often trigger this as a backup security measure when they detect "unusual activity" (like a login from a new device or location). If the line is dead, they will be locked out.
- [ ] **The "Ghost" Email Addresses:** Many of us have an old Hotmail, Yahoo, or ISP email address (****@xtra.co.nz) we rarely check but still used as the "recovery email" for our main accounts once upon a time. If your family tries to reset a password, the reset link will go to *that* old inbox. Please list **all** email addresses you possess, not just your main one, so your family doesn't hit a dead end during account recovery. Or better yet, add your trusted persons email as a backup to access your own accounts - some providers have legacy planning options.
- [ ] **The "Second Step" (Two-Factor Authentication):** Many secure accounts now require more than just a password—they ask for a code, too.
    - If you receive codes via **text message**, ensure your family has the PIN to unlock your phone.

    - If you use an **Authenticator App** (like Google or Microsoft Authenticator) or a physical **Security Key** (like a YubiKey or USB token), please note this down. Your family won't know these exist unless you tell them.

- [ ] **The Password List:** If you use a "Password Manager" app or web browser extension, write down the one "Master Password" needed to open it. If you keep your passwords in a notebook or a file, ensure your trusted person knows exactly where to find it.

Phase 2: Protecting the Money & Keeping the Lights On

This stage is about stopping unnecessary charges while ensuring critical services (and data) aren't cut off.

- [ ] **The "Do Not Cancel" List (Cloud Storage): CRITICAL:** While cancelling subscriptions, be careful **not** to cancel cloud storage services (like iCloud, Google One, Dropbox, or OneDrive) where your photos and documents are backed up. If the payment stops, these providers may **permanently delete your data** after a short grace period. Leave a note to keep these paid until the family has safely downloaded any files you wish them to keep.
- [ ] **Household Utilities:** Many utility accounts (Internet, Power, Gas) are now managed entirely via apps or email portals. Ensure your family knows which provider you use so they can transfer the account name. Otherwise, they risk the internet or power being cut off during an already difficult time.
- [ ] **Review Other Subscriptions:** Check your credit card statement for non-essential charges (Netflix, Spotify, Gym, News apps) that should be cancelled to stop the money drain.
- [ ] **Online Banking List:** You don't necessarily need to write down every banking password, but please make a list of *which* banks and institutions you hold accounts with. It is much easier for an executor to claim funds if they know where to look.
- [ ] **Digital Assets:** If you own any digital currency (like Bitcoin) or digital assets (IP, Trademarks, etc...), this is unique. If the "keys" or passcodes to these are lost, the money/asset can be gone forever and cannot be recovered by any bank or institution. Write these codes down on paper and store them securely.

Phase 3: Social Media & Online Communities

We often have "digital friends"—people we know from hobby forums, gaming groups, or online communities—who our families have never met.

- [ ] **The "Announcement" Plan:** If you have online communities you care about, your family won't know how to notify them. Consider leaving a list of these groups (or a specific friend in that group to contact) so your online friends aren't left wondering why you simply "went offline."
- [ ] **Memorialize or Delete:** For platforms like Facebook, Instagram, and LinkedIn, you generally have two choices: delete the account entirely, or "memorialize" it (where it stays up as a tribute, but no one can log in). Write down your preference.
- [ ] **Assign a Legacy Contact:** Facebook, Google and Apple allow you to nominate a "Legacy Contact"—a specific friend or family member who is given permission to manage your profile after you are gone. You can set this up in your account settings today for each platform you use.

Phase 4: Photos, Documents & Hardware

Ensuring your stories are safe and your devices go to the right home.

- [ ] **Locate the Photos:** Are your family photos on your phone? In "the cloud" (Google Photos or iCloud)? On a USB stick? Leave a simple note explaining where the most precious photos are stored so they aren't accidentally thrown away or wiped.
- [ ] **Websites & Domain Names:** If you own a personal website or domain name, these will expire and be sold to strangers if the renewal fee isn't paid. If you want a website to remain online, or the name to be kept in the family, please list the "Registrar" (e.g., GoDaddy, Namecheap) so it can be renewed, and who should inherit the domain.
- [ ] **Who Gets the Devices?** Disputes often arise over who gets to keep the iPad, the laptop, or the expensive camera. If you have specific wishes for who should inherit your physical digital devices, write this down clearly—and specify in advance if the devices should be wiped prior to the recipient receiving them—to prevent family friction.
- [ ] **The "Important" Folder:** Consider creating a folder on your computer desktop named "For Family." You can drop in important documents, contact lists for your lawyer or accountant, and perhaps even personal letters or notes you wish to leave behind.

Phase 5: Privacy and Cleaning Up

We all have things we prefer to keep private. That is okay.

- [ ] **Clear the Clutter:** If there are files, emails, or browsing histories you would prefer remain private, take the time to delete them now.
- [ ] **Instructions to Wipe:** If you have old computers or hard drives that you want destroyed or factory-reset without anyone looking at them, leave clear, written instructions to do so. Your privacy deserves to be respected.

The Legal Reality Check

To make sure your wishes can actually be carried out, there are small but vital legal steps to take.

- [ ] **The "Digital Assets" Clause:** Ask your lawyer to include a specific clause in your formal Will that gives your Executor the legal **authority** to handle your digital life. Without this, they may have the *passwords* (from this list) but not the *right* to use them. Companies may refuse to speak to them without this specific authority.

You Don't Have to Do This Alone

We understand that navigating settings menus, passwords, and security tokens can be frustrating and exhausting even at the best of times.

If you find this list overwhelming, or if you simply aren't sure how to find the settings we've mentioned, **TechHappy** is here to help. We can sit with you, patiently walk you through these steps, and handle the technical "heavy lifting" so you can focus on what matters most. We treat every session with the utmost confidentiality and care.

Please don't hesitate to reach out to us if you need a hand. Please keep yourself safe online - we **will not** reach out to you.