Securing Your Legacy in a Digital World

Do Not Let Your Digital Life Die with You

Today, so much of what once existed in material form now lives entirely online. Our photos, finances, business operations, and even our identities are stored on devices and platforms and in cloud accounts. Without proper planning, these valuable digital assets can easily be lost or become inaccessible after we die.

As a sign of the times and how deeply virtual and physical life have merged, most of us no longer distinguish between assets we can touch and those that exist only online. You cannot put cryptocurrency in your back pocket, but you can move it instantly via the phone that is in your pocket. You cannot walk into your e-commerce store, but it can generate thousands in income each month for you, and that money flows directly into your online accounts where you never physically see a dollar or cent.

Digital assets are every bit as real and valuable as traditional property—sometimes even more so. Yet many people do not treat them that way in their estate plan. Your plan may account for your home and heirlooms, but what about your Venmo balance, web domains, or crypto wallets?

A Day in the (Digital) Life

Think about how many digital assets you interact with on a daily basis. Your smartphone unlocks to reveal years' worth of photos, messages, authentication codes, and logins. You can go online to check banking and investment apps, pay bills, move money through PayPal or Venmo, and access cloud storage, subscriptions, rewards programs, and digital wallets. By day's end, you have used dozens of digital accounts, some holding real monetary value, others containing irreplaceable personal history. Yet most people do not recognize that these items are part of their overall estate.

A recent Bryn Mawr Trust survey found that Americans now place an average value of nearly $200,000 on their digital assets, and 79 percent say that protecting those assets is important—almost identical to the 78 percent who feel that way about traditional financial assets.[1] However, only 44 percent of those working with financial advisors say that the topic of digital assets and digital estate planning has ever been raised.[2]

People also underestimate the size of their digital footprint. Respondents to the same survey reported having anywhere from a handful to approximately 250 digital accounts, and many could not even estimate how many files they have.[3]

- Twenty-nine percent say they feel very or somewhat knowledgeable about digital assets.
- Twenty-one percent say they have only "a little knowledge."

---

[1] Jamie Hopkins, *Bryn Mawr Trust Survey Reveals Americans Value Digital Assets at $191,516 on Average, but Gaps Exist in Digital Asset Awareness and Estate Planning*, Bryn Mawr Tr. (Dec. 5, 2024), https://www.bmt.com/news-insights-events/bryn-mawr-trust-survey.

[2] *Id.*

[3] *Id.*

- Twenty-seven percent have heard the term *digital assets* but know almost nothing about it.
- Fifteen percent have never heard the term.[4]

If any of these findings hit home for you, you may be facing one of the major conundrums of the digital world: We constantly interact with digital assets but often have no idea what they actually are, let alone how to protect them.

So what exactly counts as a digital asset today?

Defining Digital Assets

Digital assets include any electronically stored pieces of information you own, use, control, or derive value from as well as the accounts, platforms, and devices where that information is stored. They generally fall into several categories:

- **Personal communications and media:** emails, text messages, digital photos and videos, social media profiles
- **Creative and intellectual property:** blogs, websites, domain names, digital artwork, nonfungible tokens (NFTs)
- **Financial and asset-based accounts:** online bank and brokerage accounts, crypto wallets, payment apps
- **Business and commercial digital assets:** e-commerce stores, bookkeeping and payroll platforms, monetized social media
- **Subscription and licensed digital property:** e-books, digital movies and music, gaming libraries
- **Security and authentication tools:** password managers, authenticator apps, encrypted drives
- **Records, data, and personal identity:** online statements, tax and medical portals, biometric identifiers
- **Rewards and loyalty programs:** airline miles, hotel points, credit card rewards
- **Digital memorabilia and archived content:** genealogy accounts, cloud-stored archives
- **Connected devices:** smartphones, tablets, computers, smart home devices tied to cloud accounts

Living in our digital world, differentiating between a digital asset and a traditional asset is not as obvious as it might seem. With so much of our lives now online, it is a bit like asking a fish, “What is water?” We are so immersed in digital assets, we almost do not perceive them for what they are: distinct assets that require a distinct protection plan.

How to Protect Digital Assets in Your Estate Plan

---

[4] *Id*.

Even if you understand what digital assets are, they can be easy to overlook in your estate plan. Here are some of the most common digital risks and the practical steps you can take to address them.

Not knowing what digital assets you own. Most people do not realize how much of their life runs through digital channels. Creating a complete digital asset inventory is the first step toward securing your digital legacy.

What you can do:

- Walk through a typical day, then a week, then a month.
- Write down every digital touchpoint: apps, accounts, bills, subscriptions, cloud storage, and financial platforms.
- Add these items to your digital asset inventory.

Losing access to your own digital accounts (and leaving loved ones locked out later). Without a clear plan, loved ones may never recover important digital property, from payment app balances to cryptocurrency to unused reward points.

What you can do:

- Go through each account in your digital asset inventory.
- Store access instructions (not passwords) securely.
- Let someone you trust know where your inventory and access instructions are stored.

Losing irreplaceable photos, videos, messages, and personal history. If everything lives on one device or inside a locked cloud account, your priceless memories may disappear forever.

What you can do:

- Designate Apple or Google legacy contacts to allow approved access after death.[5]
- Back up important media to a secure shared folder accessible to a spouse or trusted family member or advisor.
- Periodically review what is stored only on your phones, computers, tablets, or private accounts and move critical items to a protected backup or shared account.

Executors facing access barriers during estate settlement. Executors need access to your bills, statements, or important online documents but may be blocked without the right authority.

What you can do:

- Appoint a digital executor (or coexecutor).
- Tell your executor which accounts they may need to access during administration so they know what to look for and where to begin.

---

[5] Roger Fingas, *Who Handles Your Death Better? Google, Facebook, and Apple Compared*, Android Auth. (Jan. 16, 2022), https://www.androidauthority.com/data-after-death-google-facebook-apple-3088700.

- Ensure that your will or trust gives them explicit access rights.

Identity theft or fraud after death. Criminals often target the deceased, taking advantage of dormant accounts or publicly available probate information.

What you can do:

- Maintain an updated digital asset list so your executor knows what to secure or close quickly.
- Consider using a living trust to avoid probate court after your passing and reduce the public exposure that goes with it.
- Ensure that your executor (or digital executor) knows how to notify credit bureaus and freeze the credit file immediately after death.

Weak cybersecurity that puts your estate (and loved ones) at risk. Simple mistakes such as weak passwords, no multifactor authentication (MFA), or storing sensitive details in unprotected files create vulnerabilities now and later.

What you can do:

- Use MFA and a reputable password manager for stronger security.
- Document your MFA methods (backup codes, authenticator apps) in a secure, nonpublic place so a spouse or other trusted contact can use them in an emergency.
- Never write passwords in your will. Instead, ensure that your will or trust names a digital executor or trustee and grants them the necessary access rights.

Bring Your Digital Estate into the 21st Century

We are living in a digital world; an estate plan that is not purposefully designed to protect digital assets is incomplete and out of date.

If your estate plan has not been revisited in the past few years with an eye toward safeguarding your digital legacy, it needs attention. For help bringing your estate plan into the 21st century, schedule a time to talk with us.