

Estate Planning in the Digital Age

Help Clients Plan for Their Digital Footprint

Today, many assets that once existed in material form now live entirely online. Photos, financial accounts, business operations, and even personal identities are stored across devices, platforms, and cloud services. Without clear planning and authority, a client's digital assets can be difficult or impossible for fiduciaries or heirs to access, creating gaps in an otherwise well-structured estate plan.

Clients no longer distinguish between the assets they can physically touch and the ones that exist only online. A person cannot hold cryptocurrency in their hand, but they can transfer significant value instantly from a mobile wallet. They may never step into their e-commerce business, but it can generate substantial income for them that flows directly into digital accounts.

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

A Day in the (Digital) Life

Think about how many digital assets a typical client interacts with on a daily basis. Their smartphone is filled with years' worth of photos, messages, authentication codes, and logins. They 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, they have used dozens of digital accounts, some holding real monetary value, others containing irreplaceable personal history. Yet most clients do not recognize these items as 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 protecting those assets is important—almost identical to the 78 percent who feel that way about traditional financial assets. However, only 44 percent of those working with advisors say the topic of digital assets and digital estate planning has ever been raised.

People also underestimate the size of their digital footprint. In the same survey, respondents reported having anywhere from a handful to about 250 digital accounts, and many could not even estimate the number of files they have.

Perhaps most telling for advisors are these responses:

- Twenty-nine percent of people say they feel very or somewhat knowledgeable about digital assets.
- Twenty-one percent say they have only "a little knowledge."
- Twenty-seven percent have heard the term digital assets but know almost nothing about it.
- Fifteen percent have never heard the term.

For advisors, the message is clear: **Clients constantly interact with digital assets but often have no idea what those assets actually are, let alone how to protect them.**

So what exactly counts as a digital asset today? That may be less clear.

Defining (and Inventorying) Digital Assets

Clients (and advisors) may mistakenly believe that digital assets begin and end with Bitcoin or other cryptocurrencies; in reality, digital assets include any electronically stored piece of information a person owns, uses, controls, or derives value from, along with the accounts, platforms, and devices that store that information. 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, memberships, and loyalty programs:** airline miles, hotel points, credit card rewards
- **Digital memorabilia and archived content:** genealogy accounts, cloud-stored archives
- **Smart devices and connected technology:** smartphones, tablets, computers, smart home devices connected to cloud accounts

Most clients are unaware of how much of their life runs through digital channels until someone asks them to think about it. One effective way to start the conversation is to have clients describe a typical day and identify each digital touchpoint. Then expand the exercise: What do they access weekly? What bills autodraft monthly? Which platforms hold financial data, business information, or personal memories?

Writing down these touchpoints transforms abstract digital assets into a concrete inventory. Viewed over a day, a week, or a month, this exercise reveals accounts and information that should be documented, secured, and incorporated into an estate plan. It turns an overwhelming concept into a clear map of a client's digital estate and lays the groundwork for attorney-guided planning.

Risks, Red Flags, and Advisor Actions

Even when clients understand what digital assets are, many unintentionally leave them out of their estate plan. Advisors can watch for common risks and match each one with a simple planning step.

Risk: Permanent loss of financial value

• Red flag:

Client uses crypto, online-only banks, or payment apps with no documented access plan.

• Advisor action:

Encourage clients to inventory these accounts; securely store private keys, login credentials, and multifactor authentication (MFA) methods such as backup codes and authenticator apps in a reputable online password manager or encrypted vault; and clearly reference these records in their estate plan documents.

Risk: Executors cannot access essential digital accounts

• Red flag:

Client relies heavily on MFA, password managers, or cloud-only statements.

• Advisor action:

Recommend designating a digital executor and ensuring that their estate plan expressly grants that individual digital-access authority in accordance with state law.

Risk: Loss of sentimental or legacy information

• Red flag:

Family photos, videos, or messages exist only on a locked phone or locked cloud service.

• Advisor action:

Suggest that clients designate Apple or Google legacy contacts and back up key media in a shared secure location.

Risk: Administrative chaos during estate settlement

• Red flag:

Bills, tax documents, or monthly account or debt statements exist only in online portals no one else can find.

• Advisor action:

During your reviews with clients, walk through their daily, weekly, and monthly routines to identify where essential data is located and have them leave a digital asset list and corresponding login credentials for their executor or digital executor.

Risk: Identity theft or ongoing charges after death

• Red flag:

Dormant accounts, old email addresses, or unused subscriptions remain open.

• Advisor action:

Encourage consolidating or closing outdated accounts and maintaining an updated digital asset list.

Risk: Business disruption for owners and entrepreneurs

• Red flag:

E-commerce, domain, payroll, or customer management platforms are controlled by the client only, with no documented access or business succession plan.

• Advisor action:

Ensure that business owners document critical credentials and incorporate digital continuity into their estate plan, operating or shareholder agreements, and internal governance policies so that authorized fiduciaries can maintain operations, pay employees, and protect customer data during incapacity or after death.

Estate Planning in a Digital World

We are living in a digital world. Advisors and clients cannot overlook digital estate planning, and an estate plan that fails to address digital assets is incomplete and out of date. To bring your client's plan into the 21st century, [schedule time to talk with them, and with us](#), about protecting their digital legacy.
