Protect Your Estate from Cyberthreats

Well, that doesn't seem right.

It usually starts with something small. A strange email from a bank you do not recognize. A new credit card account you do not remember opening. A password reset link you never requested. A notice from the Internal Revenue Service (IRS) that someone has already filed a tax return in your name.

At first there is confusion. *No, there's no way that's right.*

Then anxiety sets in. *Am I being scammed?*

After that, you may spend hours or days on the phone with banks, credit bureaus, and government agencies to reach an unsettling conclusion: S*omeone has my information and is pretending to be me.*

Next comes anger, frustration, and a sense of violation. *How could this happen?*

Acceptance eventually sets in, along with a determination to never let scammers get the upper hand again. But sometimes it is too late. The damage has been done—to finances, reputation, peace of mind, and, sometimes, legacy.

Preventing cybercrimes such as identity theft starts with awareness, including the recognition that cybersecurity is not just an IT problem or something that affects businesses. It is a personal wealth preservation issue that can affect you not only now but also after you are gone, making it crucial to strengthen your digital defenses long before your estate reaches administration.

Scammers routinely target estates, executors, and grieving families, often by mining obituaries and public probate records to launch phishing, impersonation, and identity-theft schemes.

Growing Cyberthreats and Their Impact on Estate Planning

You may have started to take the first steps toward creating a digital estate plan, but that planning should also account for the growing risks that cybercriminals pose to both your assets and your legacy.

- Seventy-three percent of US adults have experienced some form of online scam or cyberattack. Most report weekly scam calls, text, and emails.[1]
- Americans reported 2.6 million fraud cases and 1.1 million identity-theft incidents to the Federal Trade Commission (FTC) in 2024. Losses exceeded $12.5 billion, a 25 percent increase over the prior year.[2]

---

[1] Jeffrey Gottfried, Eugenie Park, & Monica Anderson, *Online Scams and Attacks in America Today*, Pew Rsch. Ctr. (July 31, 2025), https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today.

[2] *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*, Fed. Trade Comm'n (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

- Identity theft is now one of the most common types of consumer fraud, with nearly 750,000 cases in the first half of 2025 alone.[3]

- Seventy-six percent of consumers say they feel more anxious about cybersecurity today than they did two years ago, driven by impersonation enabled by artificial intelligence (AI) and increasingly sophisticated scams.[4]

Cybercriminals now use AI-generated voice clones to impersonate loved ones, breached financial and medical data to answer security questions, and automated scraping of public records to target people with unnerving precision. You will very likely be targeted at some point and may have already been a victim of cybercrime. Even if you avoid direct harm during your lifetime, your estate and heirs may be more vulnerable after your death.

Why Estates Can Be Vulnerable to Cybercriminals

The FBI reports that in 2024, Americans over age 60 were the most frequently targeted demographic for online scams and fraud and lost the most money to cybercrimes.[5]

Fraud schemes targeting the estates of people who have passed away are another area of growing cybercrime concern.[6] As with older adults, estates, particularly those of seniors, are often perceived as holding substantial assets. The individuals and property involved with estate administration can also create unique vulnerabilities that attract cybercriminals.

- The loved ones left behind are often overwhelmed and distracted after a loved one's death, making them more susceptible to scams. Cybercriminals use times of chaos, confusion, and heightened emotion to their advantage, preying on feelings such as fear, urgency, and trust during times when people may let their guard down.

- Executors may be unfamiliar with digital security, making phishing attempts more successful.

- Multiple parties (attorneys, advisors, banks, beneficiaries) are exchanging sensitive documents during estate administration, sometimes through unsecured or informal methods.

- The deceased person's dormant accounts are often easy entry points for identity theft because they often go unmonitored, rely on outdated passwords, and may be tied to personal information that criminals can exploit before anyone realizes that there is a problem.

---

[3] Jack Caporal, *Identity Theft and Credit Card Fraud Statistics for 2025*, MotleyFoolMoney (Aug. 15, 2025), https://www.fool.com/money/research/identity-theft-credit-card-fraud-statistics.

[4] Vicky Hyman, *When It Comes to Fraud, a Sense of Insecurity and Even Inevitability, Global Survey Shows*, Mastercard Cybersecurity (Oct. 6, 2025), https://www.mastercard.com/us/en/news-and-trends/stories/2025/consumer-cybersecurity-survey.html.

[5] Press Release, FBI, *FBI Releases Annual Internet Crime Report* (Apr. 23, 2025), https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report.

[6] Henry Rinder, *Fraud Targeting the Elderly and Estates: A Growing Concern*, NJCPA (Sept. 23, 2024), https://www.njcpa.org/stayinformed/news/blog/post/njcpa-focus/2024/09/23/fraud-targeting-the-elderly-and-estates--a-growing-concern.

- Scammers routinely impersonate banks, government agencies, attorneys, or even the executor.
- Probate is public, giving criminals a ready-made list of heirs, contact information, and sometimes asset details.

Social engineering attacks—scams that use deception rather than technical hacking—that rely on sophisticated cybertools such as AI to exploit basic human psychology and manipulate people are on the rise.[7] And just as cybercriminals capitalize on natural disasters[8] and tech outages,[9] the estate administration process is a scenario that could provide the perfect opening for fraud and deception.

A Digital Defense Plan for Your Estate

You would not leave your physical property unsecured, but without a digital defense plan, you are essentially leaving the front door unlocked to cyberthieves, compromising your traditional and digital assets. Understanding points of vulnerability and taking a few simple precautions can help reduce your exposure to cybercrimes.

Issue: Email is the weakest link. Most cyberattacks begin with email.

- **What you can do:** Use strong passwords, multifactor authentication (MFA), and encrypted document-sharing platforms. Avoid sending unprotected sensitive materials, and encourage your executors to follow the same security practices when administering your estate.

Issue: Executors cannot secure what they cannot see. Unknown or dormant accounts often remain open and unmonitored, making them prime targets for takeover and identity theft.

- **What you can do:** Create a detailed inventory of important digital accounts and storage locations. Ensure that fiduciaries (such as your executors and advisors) know what accounts must be closed, monitored, or secured.

Issue: Sensitive legal and tax documents are insecurely stored or shared. Wills, statements, and tax documents often sit unprotected in inboxes or cloud folders.

- **What you can do:** Store documents securely using online encrypted folders or password-protected vaults, and ensure that fiduciaries know where to find documents and how to access them.

Issue: Executors may not be prepared for digital threats. Phishing attempts surge during estate administration, and many executors are unfamiliar with digital-security practices.

---

[7] Michelle Maratto & Sana Hashmat, *Unmasking Social Engineering: Protecting Your Wealth from Deceptive Cyber Tactics*, J.P. Morgan Wealth Mgmt. (Oct. 1, 2025), https://www.jpmorgan.com/insights/cybersecurity/phishing/unmasking-social-engineering-protecting-your-wealth-from-deceptive-cyber-tactics.

[8] Niamh Ancell, *Cybercriminals Capitalize on LA Wildfire Chaos via Fake GoFundMe's and Crypto Coins*, Cybernews (Jan. 17, 2025), https://cybernews.com/cybercrime/cybercriminals-exploit-la-wildfires.

[9] Brian Fung & Sean Lyngaas, *Hackers Are Already Taking Advantage of the CrowdStrike Outage Chaos*, CNN Bus. (July 22, 2024), https://www.cnn.com/2024/07/22/tech/hackers-crowdstrike-outage-scams.

- **What you can do:** Name a tech-literate executor (or coexecutor) who is comfortable managing digital accounts and security protocols. Include with your estate planning documents a brief "executor security checklist" that outlines verification steps (such as confirming account ownership and access authority) and highlights common red flags, such as urgent payment requests, unexpected account changes, or requests for credentials.

Issue: Probate exposes personal information. Public probate court filings often disclose the names and contact information of executors and beneficiaries and may even include a list of assets with their values—information that scammers can easily weaponize.

- **What you can do:** Talk with your attorney about whether trust-based planning or other probate-avoidance tools can reduce public exposure of your estate and limit targeted fraud.

Issue: Heirs and beneficiaries are prime targets for impersonation scams. Criminals impersonate banks, attorneys, courts, or even executors to solicit money or sensitive data. For example, a scammer may send an email posing as the estate's bank or attorney, claiming an urgent problem with an account and requesting immediate payment or login credentials from a beneficiary or executor.

- **What you can do:** Educate executors and beneficiaries about how to spot and avoid common scams[10] and establish a simple verification process for unexpected requests.

Issue: Identity theft of the deceased is common. Dormant and unmonitored accounts create easy entry points and are frequently hijacked after death. Criminals use a decedent's information found in public records and online obituaries to open credit accounts, redirect mail, submit false change-of-address forms, or file fraudulent tax returns.

- **What you can do:** Develop a postdeath digital and identity-protection checklist for your estate and executor. This should include promptly notifying the major credit bureaus of the death, placing a credit freeze or fraud alert on the decedent's credit file, forwarding and monitoring mail, filing the final tax return and IRS death notification, and quickly closing, consolidating, or memorializing unused online accounts and financial profiles.

Do Not Become a Cybercrime Statistic

Cybercrime statistics are sobering. We all know the risks of falling prey to online fraudsters, but when knowledge is not paired with action, it is an invitation for disaster. A proactive approach to cybersecurity rooted in awareness, preparation, and avoiding high-risk situations is key to securing your estate—and your legacy—in a digital world.

[10] *How to Avoid Imposter Scams*, Fed. Trade Comm'm Consumer Advice, https://consumer.ftc.gov/features/how-avoid-imposter-scams (last visited Dec. 22, 2025).