Be a Part of Your Clients' Digital Defense Plan

Well, that doesn't seem right.

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

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

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

After that, there may be hours or days spent 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 anymore. It is a wealth preservation issue that can affect someone's legacy even after they are gone. And for advisors, that awareness plays a central role in strengthening clients' digital defenses long before their estates ever reach 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 Can Affect Estate Planning

Consider having "the talk" with clients about cryptocurrencies and their digital estate plan if they have one. However, that talk is incomplete if it fails to cover the growing risks that their digital assets—and legacy—face from cybercriminals.

- 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. Nearly everyone will be targeted at some point if they have not already been. Even if your clients avoid direct harm during their lifetime, their estate and heirs may be more vulnerable after their death.

Why Estates Can Be Vulnerable to Cybercriminals

Older adults are particularly vulnerable to online scams and fraud due to their lower digital literacy and higher accumulated wealth. The FBI reports that in 2024, Americans over the age of 60 were the most frequently targeted group and lost the most money. [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 decedent's loved ones are often overwhelmed and distracted, making them more susceptible to realistic-sounding 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 might 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 decedent'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 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 Advisors and Their Clients

Clients count on advisors to help safeguard their wealth. In today's digital world, that includes protecting against cyberrisks that can compromise traditional and digital assets. Advisors can meaningfully reduce exposure by addressing the most common vulnerabilities before and during estate administration.

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

- **Advisor action:** Encourage strong passwords, multifactor authentication (MFA), and encrypted document-sharing platforms. Advise against sending sensitive materials unprotected and urge your clients to encourage their executors to follow the same security practices when administering the estate.

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

- **Advisor action:** Help clients build a detailed inventory of important digital accounts and storage locations. Instead of collecting credentials yourself, have your clients ensure that their fiduciaries 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.

- **Advisor action:** Encourage secure online storage using 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.

- **Advisor action:** Suggest naming a tech-literate executor (or coexecutor) who is comfortable managing digital accounts and security protocols. Have clients provide 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.

- **Advisor action:** Encourage your clients to meet with their estate planning attorney to discuss whether trust-based planning or other probate-avoidance tools can reduce public exposure and limit targeted fraud.

Issue: Heirs and beneficiaries are prime targets for impersonation scams. Criminals impersonate banks, attorneys, courts, or even the executor 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.

- **Advisor action:** Encourage clients and prospects to educate executors and beneficiaries about common scams[10] and establish a simple verification process for unexpected requests.

Issue: Identity theft of the deceased is common. Criminals use a decedent's information to open credit accounts, redirect mail, or file fraudulent tax returns.

- **Advisor action:** Provide clients with a postdeath digital checklist: notify credit bureaus, freeze credit files, and close unused accounts promptly.

Issue: Families may not know what "normal" looks like. Executors and heirs sometimes cannot distinguish legitimate communications from sophisticated scams.

- **Advisor action:** Become engaged early in the process. Encourage fiduciaries and heirs to verify all unexpected communications with you or the estate's attorney before acting.

The Best Defense Is a Good Office Visit

"The best defense is a good offense" is a truism in sports, the military, and the business world. Advisors and clients cannot confront online fraudsters in their digital hideouts, but they **can** take a proactive approach to cybersecurity rooted in awareness, preparation, and avoiding high-risk situations.

Schedule a time to talk with your clients about their digital defense plan and how you—and we—can be part of the solution.

---

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