NYLK

DIGITAL ESTATE MANAGEMENT

FREE RESOURCE · NO. 02

Locked Out

The 12 ways a digital estate falls apart — documented from real events in 2026 — and the standard that prevents every one of them.

Give your loved ones clarity — not chaos.

NYLK · nylk.com.au
Version 1.0 · July 2026 · Australia

The paradox every Australian family walks into

When someone dies in Australia, their family inherits the legal right to their digital assets — and almost no practical way to reach them. There is no federal law governing access to a deceased person's accounts. Each platform's terms of service decide, on the platform's timeline, by the platform's definition of proof. This report documents how that plays out, failure by failure.

14.2M
Email logins exposed in one June 2026 breach

52
Online games permanently shut down in 2026 so far

47 / 0
US states with digital-asset access laws vs Australia

14×
Deceased accounts less likely to be monitored for fraud

HOW TO READ THIS REPORT

Each of the twelve failures that follow has three parts: **what goes wrong**, **seen in the wild** — a documented event, most from the past twelve months — and **the standard**: the specific property a gold-standard digital estate plan has that prevents it. None of this is written to alarm you. It's written because every one of these failures is preventable, and prevention starts with knowing the failure exists.

Where the examples come from

Events referenced in this report are drawn from public reporting between mid-2025 and July 2026 — breach disclosures, platform announcements, legislation and court decisions. Full source list on the back page. Company names are used only where events were publicly reported by the organisations themselves or major news outlets.

THE TWELVE FAILURES

1 The email skeleton key

Almost every account recovery on the internet runs through email — password resets, verification links, two-factor fallbacks. An executor's first practical step is usually the deceased's inbox. If that inbox is unreachable, most of the estate is unreachable. And if it was quietly compromised before death, the executor is running recoveries through a mailbox someone else may be watching.

> SEEN IN THE WILD · JUNE 2026
>
> Japanese telco KDDI disclosed that attackers breached a shared email platform serving six internet providers, exposing up to 14.2 million email addresses and hashed passwords — one of the largest email-credential breaches on record. Every account attached to those addresses inherited the risk.

THE STANDARD The plan maps recovery paths, not just accounts: which email unlocks what, where two-factor lands, and which route an executor should use first — so email is treated as the estate's front door, and protected like one.

2 The stale password list

The most common "digital estate plan" in Australia is a handwritten list in a drawer. It's a good instinct — and it decays fast. Passwords rotate, accounts get added, banks force resets. Within six months the list is partly wrong; within two years it's a museum piece. Worse, a paper list of live credentials is a standing security risk in the meantime.

> SEEN IN THE WILD · ONGOING
>
> Estate practitioners report the same pattern on repeat: families confidently produce "the list", then discover half the entries fail — triggering lockouts on the accounts that mattered most (see Failure 10).

THE STANDARD An inventory that records what exists and how access is granted — a map, not a pile of keys — reviewed on a schedule so it's current when it's finally needed.

3 The password-manager illusion

Password managers are excellent security tools — and incomplete estate tools. They store logins, not meaning: no record of what an account is, what it's worth, or what should happen to it. Emergency-access features exist on some, but they hand over everything at once with no verification of death, no instructions attached, and no help when a platform demands proof a password can't provide.

SEEN IN THE WILD · 2026

Two major password managers disclosed breaches within a single month in mid-2026, and credential-vault compromises have recurred across the industry for years. A vault is one target holding every key — protection and concentration risk in the same product.

THE STANDARD Keep the password manager — it's good hygiene. The estate layer sits above it: inventory, per-asset instructions and a verified release process that doesn't depend on any one vendor staying breach-free.

4 The accounts nobody knew existed

Families can only recover what they can find. The average adult holds two hundred-plus online accounts; the ones that surface after a death are the ones with paper trails. The rest — old crypto exchanges, a domain renewed annually, a monetised YouTube channel, an ancient email holding the recovery keys — simply go dark. Researchers estimate the average person now holds tens of thousands of dollars in digital assets; unclaimed value at this scale is structural, not exceptional.

SEEN IN THE WILD · 2026

US reporting in 2026 highlighted actors' and creators' unclaimed residuals and dormant digital accounts surfacing years after death — value that sat undiscovered because no inventory existed. The same dynamic plays out invisibly in ordinary estates every week.

THE STANDARD Structured discovery, done while you're alive to answer questions: a professional walks your financial, creative and administrative life to surface accounts you'd never think to list in one sitting.

5 The platform that shut down first

Digital assets sit on rented land. Platforms merge, pivot and switch off — and when they do, they don't wait for probate. Data that isn't exported before the shutdown date is gone regardless of who legally owns it. An executor working through a six-month backlog can arrive at a service that stopped existing in month two.

SEEN IN THE WILD · JULY 2026

Samsung discontinued its Messages app for US users on 6 July 2026, with users reporting chat histories lost in migration. Fifty-two online games have been permanently shut down in 2026, some deleting purchased content ahead of closure. An end-of-life planning platform used by nearly two million people was itself decommissioned this year after an acquisition.

THE STANDARD The inventory records where irreplaceable data lives and flags platform risk — so exports happen before shutdowns, not after, and your family knows what needs saving first.

6 The law that never arrived

Forty-seven US states have adopted RUFADAA-style legislation giving executors legal standing over digital accounts. The UK's Property (Digital Assets etc) Act 2025 now recognises digital assets as personal property. Australia has no equivalent. Here, platform terms of service outrank a Grant of Probate — an executor can hold full legal authority and still be told no by a company in California. Apple, for instance, requires a court order for iCloud access where no Legacy Contact was set.

SEEN IN THE WILD · ONGOING

The NSW Law Reform Commission is reviewing access to digital assets after death or incapacity, with a preliminary view favouring reform — but no legislation has passed. Australia's 2026 Digital Assets Framework covers crypto exchanges, not your email, photos or socials.

THE STANDARD Plan as if the law won't save you, because today it won't: platform-native tools configured in advance, per-platform access pathways documented, and instructions that work within each platform's actual policy.

7 Ghost hacking — identity theft after death

A deceased person's accounts are a criminal's favourite kind: fully credentialed, financially connected, and watched by no one. Deceased accounts are estimated to be fourteen times less likely to be monitored than living ones. Meanwhile breached data never expires — a health record or identity document stolen years ago is still usable against an estate today, because you can reset a password but not a date of birth.

SEEN IN THE WILD · 2026

Medtronic notified 3.8 million patients in mid-2026 that names, identity numbers and health information were stolen — data that stays dangerous permanently. Security researchers documented "ghost hacking" as a growing pattern: criminals monitoring death notices, then working the deceased's accounts before families get organised.

THE STANDARD A breach-aware inventory: which identities are known-compromised, which accounts need protecting rather than just accessing, and a defined first-week protocol so the estate is secured faster than it can be exploited.

8 Crypto that dies with its keys

Self-custodied crypto is the only asset class with no recovery mechanism at all. No court order retrieves a seed phrase. Exchange accounts are little better in practice — succession processes vary wildly between platforms, and Australia's new licensing framework regulates the exchanges, not your family's access. Researchers estimate hundreds of billions of dollars in cryptocurrency is already permanently stranded in inaccessible wallets worldwide.

SEEN IN THE WILD · ONGOING

The pattern repeats publicly every year: holdings visible on-chain, families certain the assets exist, and no path to them — because the one person who knew the access method is gone.

THE STANDARD Custody documented asset-by-asset: what exists, how it's held, and a secure access arrangement for keys that doesn't require storing them with the plan itself. Designed once, tested, and kept current.

9 The business that stops on Monday

For an owner-operated business, the digital estate is the business: the accounting file, the domain, the payment gateway, the ad accounts, the client records. A shareholders' agreement handles equity — it does not hand anyone the Xero login. When the one person holding admin access is suddenly gone, invoicing stops, renewals lapse, ads keep spending, and staff can't even reach the systems that pay them.

SEEN IN THE WILD · ONGOING

Business insurers and accountants describe the same first fortnight after a key-person loss: a scramble to reconstruct access from receipts and inboxes while the business bleeds value daily. Employer-side breaches (like the Oracle HR-system attacks disclosed in June 2026) add another layer — records an executor needs may already be compromised.

THE STANDARD

A business continuity tier: every operational account inventoried with named delegates, so the business can run on Monday no matter what Sunday held.

10 The two-factor deadlock

Two-factor authentication is designed to stop anyone who isn't you — and after death, that includes your family. The commonest deadlock: the right password, entered correctly, defeated by a code sent to a locked phone. Repeated attempts trigger security lockouts that convert a solvable problem into a permanent one. The phone passcode, the 2FA app and the backup codes are the estate's real master keys, and they're the items least often planned for.

SEEN IN THE WILD · ONGOING

Families routinely cancel the deceased's phone plan in week one to save money — severing SMS-based two-factor for every account at once, before anyone realises what the number was still guarding.

THE STANDARD

The plan treats devices and second factors as first-class assets: passcode escrow arrangements, backup codes stored securely, and an explicit "do not cancel yet" list for the first ninety days.

11 The subscription bleed

The average Australian carries a dozen or more active subscriptions — streaming, software, storage, memberships — most on auto-renew against a card that keeps working after its owner doesn't. Estates commonly leak around $2,400 a year this way while administration grinds on, and every cancellation requires its own death-verification dance with a different provider.

SEEN IN THE WILD · ONGOING

Executors report subscriptions surfacing for a year or more after death — annual renewals are the worst offenders, billing once, quietly, eleven months after everyone thought the list was complete.

THE STANDARD Subscriptions inventoried with billing dates and cancellation paths, so the estate stops the bleed in week one instead of discovering it at tax time.

12 The plan that was never finished

The quiet failure behind all the others. DIY digital estate tools assume you'll do the work: fill the vault, write the instructions, keep it current, forever. Most people start, feel organised, and stop at 30% complete — leaving a plan that looks like protection and functions like false confidence. A plan's value is set by its weakest unfinished section.

SEEN IN THE WILD · INDUSTRY-WIDE

Self-serve platforms in this category publicly battle completion rates — the product works; unaided humans don't finish. It's the same reason most wills in Australia are drafted with a professional, not from a kit.

THE STANDARD The plan is built *with* you by a professional, to a defined standard of done — then reviewed annually so "finished" stays true. You shouldn't have to become an estate administrator to be ready for one.

What the gold standard actually looks like

Twelve failures, one pattern: plans fail where they're static, partial, or unverified. Hold any solution — including ours — to these six tests. This is the standard NYLK built its Digital Directive service to meet.

THE TEST	WILL ALONE	PASSWORD MANAGER	DIY DIGITAL VAULT	GOLD STANDARD (NYLK DIGITAL DIRECTIVE)
Complete discovery — every account found, not just the memorable ones	—	—	Partial	✓
Context & instructions — what each asset is and what should happen to it	Partial	—	Partial	✓
Verified release — access granted only on verified death or incapacity	—	—	Partial	✓
Kept current — reviewed with a human on a schedule	—	—	—	✓
Breach & platform awareness — knows what's compromised and what's at risk of vanishing	—	—	—	✓
Built for Australia — local operations, local law, local platforms	✓	—	—	✓

"Partial" reflects typical capability of the category, not any single product. Your will remains essential — a Digital Directive complements legal estate planning, it never replaces it.

Hold your plan to the standard

Take the free Digital Estate Readiness Scorecard, or start with the 47-Account Inventory — free at nylk.com.au

NYLK.COM.AU

Sources: KDDI breach disclosure via BleepingComputer & Security Affairs, June 2026 · Medtronic patient notifications via SecurityWeek & HIPAA Journal, 2026 · Samsung Messages discontinuation via CNET & Android Police, July 2026 · 2026 game shutdowns via GameRant · Oracle PeopleSoft zero-day HR breach via BleepingComputer, June 2026 · RUFADAA adoption via Thomson Reuters Practical Law state chart & Trust & Will 2026 Estate Planning Report · UK Property (Digital Assets etc) Act 2025, parliament.uk · NSW Law Reform Commission digital assets review · Australian Digital Assets Framework, 2026 · deceased-account fraud monitoring and subscription-leakage figures: NYLK research library, 2026. General information only — not legal or financial advice.

Your Legacy. Poured Forward.