Max Paradox

**PROBLEM? RELAX. YOU'VE GOT THIS!**

A tongue-in-cheek guide series ;)

# A Loved One Left Behind a Phone, the Cloud, and a Hundred Passwords

How to Prepare Access to Photos and Important Accounts, Organize a Loved One's Digital Affairs, and Know What Can Be Closed, Recovered, or Kept Without Playing Digital Detective at the Worst Possible Time



**We have a problem. But relax.**

It can be solved—and we might even have a laugh along the way.

# A Loved One Left Behind a Phone, the Cloud, and a Hundred Passwords

## How to Prepare Access to Photos and Important Accounts, Organize a Loved One's Digital Affairs, and Know What Can Be Closed, Recovered, or Kept Without Playing Digital Detective at the Worst Possible Time

Max Paradox

PROBLEM? RELAX. YOU'VE GOT THIS!

ISBN: 978-83-8483-730-6

# CONTENTS

INTRO ..... 5

Chapter 1 - The Digital Life That Never Received the News ..... 11

Chapter 2 - Knowing the Password Is Not the Same as Having Permission ..... 20

Chapter 3 - The Photos Are Somewhere. Unfortunately, Somewhere Is Not an Address ..... 29

Chapter 4 - The Subscriptions Have Not Been Told to Stop Charging ..... 38

Chapter 5 - Before You Press Reset, Find Out What Reset Actually Means ..... 49

Chapter 6 - A Hundred Passwords and the One Missing Piece That Locks Everything ..... 58

Chapter 7 - The Internet Still Remembers, Even When Nobody Asked It To ..... 69

Chapter 8 - Your Loved One's Computer May Contain Somebody Else's Secrets ..... 79

Chapter 9 - The Emergency Folder That People Can Actually Understand ..... 90

Chapter 10 - How to Contact a Service Provider Without Becoming Best Friends with a Chatbot ..... 99

Chapter 11 - One Missing Document, a Thousand Unnecessary Searches ..... 110

Chapter 12 - Closing an Account Without Accidentally Closing Everything Else ..... 120

Chapter 13 - The Money That Exists Online but Never Appears in a Wallet ..... 131

Chapter 14 - Don't Give Your Family an Entire Hard Drive. Give Them Memories They Can Find ..... 141

Chapter 15 - When Something Cannot Be Recovered, No Matter How Much You Want It Back ..... 152

Chapter 16 - When Everybody Has Advice but Only One Person Has the Work ..... 163

Chapter 17 - When Scammers Offer to Recover Everything, Including Your Money ..... 174

Chapter 18 - Keeping Digital Affairs in Order Without Making Them Your Second Job ..... 184

Chapter 19 - Helping Someone Before They Can No Longer Help Themselves ..... 195

Chapter 20 - Leave Your Family a Way Forward, Not a Digital Treasure Hunt ..... 206

# INTRO

The email arrived on a Thursday morning, three days after the funeral. “Great news! Your subscription has been renewed successfully!” Under different circumstances, this might have been a perfectly ordinary message. Unfortunately, the subscription belonged to Daniel, who had died the previous week, and the person reading it was his sister, Rebecca. She had been trying to find the photographs he took during their last family holiday. Instead, she had discovered three email addresses, two cloud storage services, a laptop that refused to cooperate, and a collection of passwords that appeared to have been invented by a committee of particularly suspicious mathematicians. The subscription company, meanwhile, was delighted. Its customer retention strategy was apparently performing beyond the usual boundaries of human existence.

Nobody tells you that losing someone may also mean becoming the temporary administrator of an entire digital universe. There are obvious responsibilities after a death, and then there are the invisible ones: online accounts, automatic payments, photographs, documents, social media profiles, digital purchases, and services that quietly continue operating. Some contain precious memories. Others contain important information. A surprising number exist because somebody once needed a free trial, forgot to cancel it, and subsequently financed the continued operation of an application they opened exactly twice. Sorting through this collection can feel overwhelming, particularly when you are already dealing with grief, family responsibilities, paperwork, and the exhausting business of answering people who ask whether there is anything they can do to help.

The trouble is that our digital lives rarely come with an instruction manual. We build them gradually, over years, without noticing how complicated they have become. One email address opens the way to another account. A phone approves sign-in requests. A password manager protects dozens of passwords behind a single set of credentials. Photographs appear automatically on different devices, encouraging the comforting belief that they must be safely stored somewhere. Everything seems beautifully connected until the person who understands those connections is no longer available. Then the technology starts asking questions that nobody else can answer, usually beginning with “Please verify that you are the account owner.” An excellent security precaution, admittedly, but not a particularly helpful conversation starter under the circumstances.

It is tempting to approach the whole problem as a technical challenge. Find the passwords, unlock the devices, copy the files, close the accounts, and declare victory. Unfortunately, that approach overlooks several important complications. Having someone's phone does not necessarily give you the right to access their private communications. Knowing a password does not automatically authorize you to use an account. Canceling a service may affect information stored within it, while deleting an account can sometimes have consequences that cannot easily be reversed. And the photographs that look safely backed up might turn out to be synchronized copies, meaning that an innocent attempt to tidy up one device could affect the contents of another.

There is also an enormous difference between discovering that something exists and knowing what should

happen to it. A forgotten entertainment subscription, an investment account, a family photograph collection, and a confidential work document do not belong in the same decision-making category. Some matters need prompt attention because deadlines or financial consequences are involved. Others need careful preservation. Some require official procedures, appropriate documentation, or specialist advice. And quite a few can be left alone without anyone suffering the slightest inconvenience. The aim is not to become the world's most determined digital detective. It is to identify what matters, understand your options, and avoid making a difficult situation worse through perfectly understandable haste.

This book is written for two kinds of readers who have more in common than they might initially imagine. The first is someone dealing with the digital affairs of a loved one who has died or can no longer manage certain matters independently. Perhaps you need a document, want to preserve family memories, or are trying to understand which accounts require attention. You may have spent hours searching for straightforward instructions and discovered that every website has a different procedure. The second reader is someone who would rather prevent that situation from becoming unnecessarily complicated in the first place. You have your own accounts, devices, photographs, and important information, and you would like the people you trust to have a reasonable chance of finding what they genuinely need.

If you belong to the second group, there is encouraging news: preparing your digital affairs does not require turning your home into a miniature cybersecurity headquarters. You do not need to print every password, purchase an industrial-

strength safe, or appoint your most technically enthusiastic relative as Supreme Commander of Family Information Technology. You need a sensible understanding of your important services, secure arrangements for information that should be available to authorized people, and clear decisions about what you want preserved or handled in particular circumstances. The right solution might involve official legacy-access features, carefully organized documents, appropriately shared family resources, or formal arrangements that match your situation. It should also respect the things you prefer to keep private.

If you are already managing someone's affairs, the priorities are different. You may have little information and even less energy. You may encounter a device that cannot be unlocked, an account provider that cannot release certain data, or a service whose rules are more complicated than the problem you originally wanted to solve. This book will help you distinguish between practical actions, technical limitations, and questions that require legal or professional guidance. It will not promise universal account recovery, miraculous access to encrypted devices, or guaranteed solutions to disputes. Anyone offering those things with suspicious enthusiasm deserves careful scrutiny, especially if their next sentence involves an urgent payment and an unusually convenient bank transfer.

We will also pay attention to something that technical instructions frequently overlook: the emotional value of ordinary digital material. A short voice recording, an unremarkable photograph, or an old message can mean far more than a perfectly organized collection of official documents. Someone may urgently want to recover those memories. Someone else may need months before feeling

ready to look at them. Neither response is a problem to be corrected with better folder management. Practical responsibilities may have deadlines, but grief does not come with a progress bar, and there is no award for completing all of a loved one's digital administration before the weekend.

Throughout these pages, the guiding question will be simple: what is the next responsible action that actually helps? Sometimes it will involve gathering reliable information. Sometimes it will mean contacting a service provider, checking what an account closure would affect, or arranging access to material you are entitled to preserve. Occasionally the best decision will be to stop before pressing a button whose consequences you do not understand. We will distinguish what can be closed, what may be recovered, what deserves to be kept, and what should remain private. There will be practical examples, explanations without unnecessary technical jargon, and a reasonable amount of amusement directed at systems that insist on being spectacularly unhelpful at precisely the wrong moment.

Above all, you do not have to solve everything. Nobody's digital life is perfectly documented, and even the most careful preparations cannot anticipate every future change in technology, service rules, or family circumstances. The goal is a manageable set of decisions that reduces confusion, protects valuable information, and gives the right people a clearer way forward. Where legal rights, financial responsibilities, or sensitive information are involved, general guidance cannot replace the appropriate official process or individual professional advice.

One day, somebody may inherit the practical task of dealing with your devices and accounts. Or perhaps you are

already facing that responsibility for someone you love. Either way, the most useful thing you can have is not a hundred passwords scribbled on the back of an envelope. It is enough understanding to know what matters, where to begin, and when to ask for the right help.

The people we love leave behind stories, relationships, memories, and traces of ordinary life. Their phones and online accounts are merely some of the places where those traces happen to be stored. Technology ought to help us preserve what matters, not turn remembrance into an obstacle course with mandatory two-factor authentication.

And if we can prevent somebody from having to solve a password puzzle while navigating one of the hardest moments of their life, that is already a very worthwhile achievement.

# Chapter 1 - The Digital Life That Never Received the News

The smart doorbell still recognized Oliver as the owner of the house. Six weeks after his death, it continued sending notifications to his phone, saving recordings to his online account, and treating everyone else as an occasional visitor. His daughter, Hannah, discovered this when she tried to help her mother change the settings. The device worked perfectly. It recorded visitors, announced deliveries, and provided an excellent view of the neighbor's cat conducting its daily inspection of the front steps. Unfortunately, nobody in the family knew who could administer it. Oliver had installed the system, registered the account, and apparently appointed himself permanent Minister of Front Door Technology. His absence had not been included in the manufacturer's operational assumptions.

The doorbell was only the beginning. A tablet controlled some of the lights, an unfamiliar online service stored household documents, and a personal email address appeared on various contracts. Oliver had also maintained the website of a local gardening club, although nobody could explain why the club's membership records were connected to his private laptop. Every discovery raised two further questions. Hannah initially thought she needed to find the passwords, but gradually realized that she did not even know what she needed them for. The family had inherited a collection of functioning digital arrangements without inheriting the knowledge that held those arrangements together.

This is the peculiar nature of a person's digital life. It does not exist in one place, and it does not stop functioning simply because its owner is no longer available. Instead, it consists of devices, accounts, information, subscriptions, permissions, and relationships between services. Some elements hold irreplaceable memories. Others support ordinary household activities. A few may have financial or legal consequences. Many are completely unimportant, apart from their remarkable ability to generate notifications. Understanding this collection is the first step toward managing it responsibly. Trying to control everything before understanding anything usually creates additional confusion, which is an impressive achievement when the original situation already feels like a technological escape room.

The difference between owning a device and understanding its contents

People often use the word "account" to describe several different things. Someone might say that a loved one's photographs are "on the computer", although the computer displays images retrieved from an online service. A banking application might appear on a phone, but the account itself is maintained by a financial institution. A purchased digital book might be accessible through a particular platform without being transferable to another person. These distinctions matter because the physical object, the online service, and the rights associated with its contents may be governed by different rules.

Imagine three items sitting on a desk: an external drive, a smartphone, and a printed invoice for online storage. They look like three separate objects, yet they might all relate to the same collection of photographs. Alternatively, each could point to a completely different set of files. Until the

relationship is understood, declaring the photographs either safely preserved or permanently lost would be premature. The invoice proves that a service was used or billed at a particular time. It does not prove what was stored there, whether the account remains active, or whether an authorized person can obtain its contents.

A useful distinction is between what someone possessed, what someone used, and what someone had authority to manage. Ownership of a laptop does not necessarily settle rights concerning confidential business documents stored on it. Being the administrator of a community website does not necessarily make its contents personal property. A shared household subscription may have several users but only one contractual account holder. These differences can become particularly important after death, when certain powers and arrangements may change under applicable law. The exact rules depend on the jurisdiction, the service, and the circumstances. A family member's practical responsibility to organize affairs should never be mistaken for unrestricted permission to enter every account.

For this reason, the most useful first document is usually an inventory of known digital matters rather than a list of passwords. Hannah began with information she could obtain legitimately: household paperwork, correspondence addressed to her, invoices available through proper channels, and details her mother already knew. She noted the name of each service, its apparent purpose, the source of that information, and any unresolved questions. She did not need to open Oliver's private messages or impersonate him online. At this stage, the aim was to describe the landscape, not cross every boundary within it.

There is a small but crucial difference between writing "Oliver stored everything with this company" and "We found an annual payment to this company; the contents of the account are unknown." The first statement feels reassuring, but may rest entirely on guesswork. The second is less satisfying and considerably more useful. It identifies a fact and leaves room for investigation through an appropriate procedure. In family conversations, guesses have a remarkable ability to acquire authority. One person says something might be true, another repeats it with slightly greater confidence, and by the following weekend everyone remembers that it was definitely established by Oliver himself.

Keeping facts and assumptions separate prevents this gradual transformation of uncertainty into family folklore. It also protects against unnecessary action. A relative may remember that somebody once used a particular cloud provider, but that memory alone does not justify requesting broad account access. A payment record may show that a service existed without proving an outstanding obligation. Reliable information gives each subsequent decision a foundation. Unreliable information should remain a question until it can be checked.

Some things matter more than others

Once the family had a clearer picture, Hannah faced a different difficulty. The inventory contained more entries than anyone had expected, and looking at the entire collection was exhausting. Should they investigate an old online marketplace account? What about the gardening website? Was the smart doorbell important? Did anyone need to preserve the settings of a weather station that had apparently spent five years reporting conditions from behind

the garage? The temptation was to work through everything alphabetically. It would have been beautifully organized and spectacularly inefficient.

Priority depends on consequences, not the order in which accounts are discovered. An urgent matter may involve a deadline, a potentially significant payment, a security risk, or information needed for formal proceedings. Another item may deserve attention because it holds something irreplaceable. A third might be worth understanding eventually but cause no meaningful difficulty if left alone for several months. Before spending time on a service, ask what could happen if no action were taken immediately. If nobody can identify a plausible consequence, the apparent urgency may simply be a feeling created by an unfinished list.

Hannah discovered that the gardening club website needed fairly prompt attention because members were still relying on it for current information. That did not mean she should log into Oliver's account and assume his administrator role. It meant the club needed to identify its authorized representatives and seek an appropriate route to ongoing management. The smart doorbell was useful to her mother, but its continued operation did not justify experimenting with settings before establishing what the manufacturer permitted. The weather station, meanwhile, could remain exactly where it was. The neighborhood would survive a temporary shortage of hyperlocal atmospheric statistics.

Information with emotional value requires a different kind of attention. A family may care deeply about a collection of voice recordings without needing to listen to them immediately. Someone might want reassurance that important photographs are preserved while feeling unable to

look at them. An account can therefore be significant without every associated task being urgent. Separating the need to protect something from the need to use it allows the family to respond thoughtfully. Otherwise, people can find themselves sorting intimate memories at midnight simply because the item was next on a spreadsheet.

Financial and contractual questions introduce additional considerations. An online payment service may need formal attention, but seeing its name on a screen does not establish the amount of money involved or who may receive information about it. A recurring charge may deserve investigation without necessarily justifying immediate cancellation. Where financial obligations, inheritance, privacy, or other legal rights are concerned, official procedures and appropriate professional advice can be essential. The inventory should help identify where such assistance is needed. It should not attempt to replace legal decisions with creative use of somebody else's remembered password.

The hidden relationships between accounts

One of the more confusing features of a digital life is that its components depend on one another. A telephone number may be used for verification by several services. An email address may receive notices concerning important agreements. A single online identity may provide access to applications that appear unrelated. These relationships are often invisible to ordinary users because they work quietly in the background. Trouble begins when someone changes or closes one service without realizing that several others depend upon it.

Consider an apparently unnecessary email account. The family may see no reason to preserve it, especially if nobody

is entitled to read its private contents. Yet it might have been used as the registered contact address for household services. This does not mean the family should take over the mailbox. It means that, before considering changes that affect it, they should identify important organizations and use their legitimate procedures to update relevant contact arrangements where permitted. The practical need is continued communication with the right people, not unrestricted access to years of personal correspondence.

The same reasoning applies to devices. A tablet may function as a controller for several household systems, while a phone may be registered as a trusted device for account verification. Resetting or disposing of such equipment without understanding the consequences can create avoidable difficulties. Conversely, retaining every outdated device forever is not necessarily useful. The purpose of the inventory is to identify meaningful dependencies so that later decisions can be made with an understanding of what might be affected.

Digital information also has different levels of reliability. A photograph visible in an application might be stored locally, remotely, or in both places. A scheduled online post might appear after its creator's death without indicating that anyone has accessed the account. A service notification might continue because no change has been recorded by the provider. These observations should not automatically become dramatic theories about missing data or suspicious activity. Sometimes an unexpected digital event genuinely requires investigation. Sometimes it is simply software doing precisely what it was programmed to do, with all the emotional intelligence of a parking meter.

An inventory is a map, not a promise to explore everything

A practical inventory should remain manageable. It needs enough information to support decisions, but not so much that maintaining it becomes another full-time occupation. The most useful entries identify a service or device, explain why it may matter, distinguish confirmed facts from uncertainty, and indicate whether a particular action or professional contact is required. Sensitive credentials generally do not belong in an ordinary family inventory. If some information requires separate protection, that distinction should be respected from the beginning.

The inventory also needs an owner in the organizational sense: somebody who keeps track of what has been established and which questions remain open. That person does not automatically acquire authority over the accounts themselves. They simply prevent several relatives from unknowingly duplicating work or acting on contradictory assumptions. Where family members disagree about who is entitled to make decisions, those disagreements must be resolved appropriately rather than settled by whoever happens to have the fastest internet connection.

If you are preparing your own affairs rather than handling someone else's, this exercise reveals an uncomfortable truth. You probably remember the services you use frequently, but not every arrangement that depends on you. Think of the accounts through which important household responsibilities pass, the information only you know how to locate, and the people who might need to continue a legitimate task if you became unavailable. You need not reveal private information indiscriminately. Simply identifying these dependencies can show where clearer instructions,

proper authorizations, or more suitable shared arrangements would help.

By the end of Hannah's first inventory, the family still had unanswered questions. Several services remained unidentified, and the gardening club had to make its own arrangements. Yet the situation had changed substantially. They could distinguish genuinely important matters from digital clutter, recognize where they lacked authority, and avoid altering systems whose dependencies they did not understand. Hannah had not become the new owner of Oliver's entire online existence. She had something more useful: a clear understanding of which matters required responsible attention.

That is what an inventory is supposed to achieve. It does not eliminate uncertainty, open locked accounts, or guarantee the recovery of valuable information. It replaces one enormous, shapeless problem with a collection of questions that can be addressed individually. And when the investigation is complete enough, you are allowed to stop. Nobody should have to account for every abandoned app and experimental online registration a person accumulated over decades. Some digital mysteries can remain mysteries without anyone losing sleep over them.

Oliver's doorbell continued recording visitors while the family worked through the necessary arrangements. The neighbor's cat remained its most dependable performer. The technology had not suddenly become considerate, but the family no longer expected it to understand their circumstances. They understood enough about the technology to make better decisions themselves, which was an altogether more realistic achievement.

# Chapter 2 - Knowing the Password Is Not the Same as Having Permission

There is a sentence that can transform a difficult family discussion into a surprisingly complicated legal and ethical problem: "Don't worry, I know the password." It sounds reassuring. Somebody has found a way past the first obstacle, and surely that must count as progress. Yet a password answers only one question: whether a particular piece of information may satisfy a technical authentication system. It does not explain who is entitled to use the account, what they may do with its contents, or whether that entitlement still exists under the present circumstances. A password is rather like a key found in somebody's coat pocket. Its existence tells you that a lock can potentially be opened. It does not settle whether you are allowed to enter the room.

Imagine that Margaret regularly asked her nephew, Ethan, to help with her tablet. She trusted him, and on several occasions she gave him the passcode so that he could adjust the display settings or solve a printing problem. After Margaret's death, Ethan remembered the code and offered to investigate her online accounts for the family. He genuinely wanted to help. Unfortunately, he had jumped from one limited form of permission to a much broader assumption. Margaret had allowed him to assist with particular technical tasks while she was alive. That did not necessarily authorize him to examine her personal messages, manage her finances, or take over her accounts after her death. The difference matters even when everyone involved has entirely decent intentions.

Technology makes this confusion remarkably easy. A device may open without displaying any explanation of the user's rights. An application may remember a previous login and reveal information without requesting another password. A browser may contain saved credentials for numerous services. In each case, the interface creates the impression that access is available, and people naturally associate availability with permission. But technical convenience is not a reliable guide to legal authority. A shop with an unlocked door does not automatically invite visitors to reorganize the stockroom. Nor does a computer with an active email session turn every person standing nearby into an authorized correspondence manager.

Authentication proves less than people think

Authentication is the process by which a system checks whether somebody can provide the credentials or other evidence it requires. Authorization concerns what a person is permitted to do. The two concepts often operate together, but they are not interchangeable. An account owner who signs in successfully may receive permission to perform certain actions under the service agreement. Another person possessing the owner's credentials does not necessarily acquire those permissions. The provider's rules, applicable law, and any valid authority granted to that person may all be relevant.

It is useful to distinguish several layers that often become mixed together. One concerns ownership or lawful possession of a device. Another concerns the contractual relationship between a person and an online service. A third concerns rights to particular information or digital materials. A fourth involves the privacy and interests of other people whose information appears within the account. These layers

can produce different answers. A family may lawfully possess a laptop without being entitled to inspect confidential employment records stored on it. Someone may have a legitimate need for a specific document without having any right to read years of private correspondence.

Consider a shared family computer. Several people may have used it over the years, leaving documents and active accounts in the same operating system. If one person dies, the remaining users may still need their own files and services. But that ordinary need does not provide unlimited authority over the deceased person's private information. A sensible response distinguishes genuinely shared resources from individual accounts and seeks a lawful way of dealing with each. Simply announcing that "it's the family computer" settles very little, except perhaps who gets to argue about the printer.

Privacy also extends beyond the account holder. Private messages contain words written by correspondents who may never have expected their conversations to be inspected by relatives. Documents can include information about colleagues, clients, friends, or children. Even if access to certain records is legally permitted, it may be appropriate to limit the examination to what a particular task requires. Curiosity is understandable, especially when relatives encounter unfamiliar names or unexplained accounts. But curiosity alone is not a sound reason to investigate every personal detail someone left behind.

What exactly are you trying to achieve?

Before requesting access, it helps to describe the desired outcome without mentioning a password. Perhaps the family needs a warranty document, confirmation of an outstanding obligation, or an authorized copy of particular photographs.