BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Digital Legacy

Planning ahead for your accounts and photos — and what to do for a loved one's after a death, in plain English

A gentle, practical guide for you and your family

One calm step at a time — there's no rush

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

Apple, Google, Facebook, Microsoft & password managers · facts current November 2026

What's Inside

This is your digital legacy guide. It has two halves. The first helps you plan ahead, so the people you love can reach your photos, messages and important accounts when the time comes. The second is for a family that has just lost someone: what to do first, what can wait, and how to close or keep each account gently and safely. Read it in any order and at your own pace. Nothing here is legal advice; an estate attorney handles the legal side, and this guide handles the technology.

Part 1 — Why This Matters

1 A Note from Bill
2 What a "Digital Legacy" Is
3 What Happens When No One Plans

Part 2 — Taking Stock

4 Making Your Digital Inventory
5 The Keys That Matter Most
6 Two-Factor Sign-In and the Phone Number Problem
7 Where to Keep It All Safely

Part 3 — Setting It Up, Company by Company

8 Apple: Adding a Legacy Contact
9 Google: The Inactive Account Manager
10 Facebook & Instagram: Memorial or Goodbye
11 Microsoft, Amazon & Accounts Without a Tool
12 Password Managers: Emergency Access

Part 4 — Photos, Memories & Your Wishes

13 Making Sure the Photos Survive
14 Writing Down Your Wishes

Part 5 — When Someone Has Died

15 The First Days: What to Do and What Can Wait
16 Protecting Their Identity
17 Mail, the Phone Line & Subscriptions

Part 6 — Their Accounts & Devices

18 Their Apple Account
19 Their Google Account
20 Facebook, Instagram, Microsoft, Amazon & the Rest
21 Saving the Photos From Their Phone & Computer

22 Their Devices: Keep, Pass On or Wipe

Part 7 — Staying Safe in a Hard Time

23 Scams That Target Grieving Families
24 An Obituary That Doesn't Help Thieves

Part 8 — When to Call Bill & Your Cheat-Sheet

25 When to Call Bill
26 Your Digital Legacy Cheat-Sheet

PART 1

Why This Matters

What a "digital legacy" is, what happens when nobody plans for it, and why a little preparation now is one of the kindest gifts you can leave your family.

CHAPTER 1

A Note from Bill

Hello, and thank you for opening this guide. I know it isn't the cheeriest subject. Some of you are reading because you're the planning sort and want your affairs in order. Some of you are reading because someone you love has just died, and you're facing a phone you can't unlock and a pile of accounts you don't know how to handle. Whichever brought you here, you're welcome, and you're in good hands.

I'm Bill. For more than 30 years I've helped people with their technology, and these days I do it for families here in Portage County, Ohio. I wrote this guide the way I'd talk with you at your kitchen table: slowly, in plain English, with no jargon and no pressure.

Two halves, one purpose

The first half of this guide is about **planning ahead**. It shows you how to make a simple list of your accounts, where to keep it, and how to use the free tools Apple, Google, Facebook and the password managers now offer, so the right person can reach your photos and messages after you're gone, without a court order and without guessing.

The second half is for **after a death**. It walks a family through the first days, protecting the person's identity, stopping bills and subscriptions, saving the photos, and closing or memorializing each account. It's written gently, because I know the person reading it may be grieving.

WHAT THIS DOES FOR YOU

Why this matters

A phone passcode and a few account settings can be the difference between a family that keeps every photo of Grandma and a family that loses them. Thirty minutes of planning now saves your loved ones weeks of phone calls and paperwork later, at the hardest time of their lives.

What this guide is, and what it isn't

This is a technology guide. It is **not legal advice**, and I'm not a lawyer. Wills, executors, probate and who legally inherits what are questions for an estate attorney. What I can do is show you the buttons, the settings and the forms, and help you understand what each company will and won't do.

And I'm only a phone call away

If any of this feels like too much, you don't have to do it alone. Call me at **(330) 200-8042**. Whether you want help setting up your own plan or you need someone patient to sit beside you with a loved one's phone, I'm glad to help. Take a breath. We'll go one step at a time.

— Bill

CHAPTER 2

What a "Digital Legacy" Is

Your **digital legacy** is simply everything you have online or on a device that someone might need, or want, after you're gone. It's the modern version of the shoebox of letters and the folder of bank statements in the desk drawer.

The things most families care about

- **Photos and videos** — on phones, in iCloud or Google Photos, on computers and old memory cards. For most families, these are what matter most.
- **Email** — the place where bills, statements and password resets arrive.
- **Money accounts** — online banking, investment and retirement accounts, PayPal and similar.
- **Bills and subscriptions** — streaming services, cloud storage, phone plans, newspapers, apps, Amazon Prime. These keep charging a card until someone stops them.
- **Social media** — Facebook, Instagram and others, where friends may want to share memories.
- **Devices** — phones, tablets, computers and smart-home gadgets, each locked with its own passcode.
- **Documents and notes** — recipes, family history, letters, health records and anything saved in the cloud.

Why it's harder than a paper shoebox

With paper, a family member could simply open the drawer. With technology, nearly everything is locked, and it's locked *on purpose*. Passcodes, encryption and two-factor sign-in are what keep thieves out while you're alive. The trouble is that the same locks keep your family out, too, unless you've left them a key or named them in the company's own planning tool.

GOOD TO KNOW

A new word: encryption

Encryption means scrambling information so it can only be read with the right key, like a passcode. Modern iPhones and Android phones encrypt everything on them. That's wonderful for your privacy, and it's also why a phone with an unknown passcode usually can't be opened by anyone, including the company that made it.

Your legacy is more than passwords

Planning isn't only about handing over passwords. It's also about telling your family what you *want*: which photos to keep, whether you'd like your Facebook page kept up as a memorial or taken down, who should get your computer, and which accounts can simply be closed. Those wishes are a gift in themselves.

CHAPTER 3

What Happens When No One Plans

I want to be honest about this, not to frighten you but so you understand why the planning chapters are worth your time. Here's what families commonly run into when there's no plan.

The locked phone

If nobody knows the phone's passcode, the photos and messages that live only on that phone may be out of reach for good. Apple says plainly that it can't remove a passcode lock without erasing the device. A family can often still get the *cloud* copies of photos with the right paperwork, but only if the phone was backing them up.

The account the company won't open

Big companies protect privacy very seriously. Without a planning tool set up in advance, many will only release a person's email or files with a **court order**, and even then they don't promise to help. Microsoft, for example, says it must be formally served with a valid subpoena or court order before it will even consider releasing a deceased person's email or OneDrive files.

The bills that keep coming

Subscriptions charge automatically. If nobody knows which services were being paid, small charges can keep coming out of an account for months until someone spots them on a statement.

The accounts that disappear

Some companies delete accounts after a long stretch of no use. Google says it may delete an account that's been inactive across Google for at least two years. Microsoft says Outlook.com and OneDrive accounts are frozen after one year without use, the email and files are deleted shortly after, and the account itself expires after two years. If the only copy of a photo was in one of those accounts, waiting too long can mean losing it.

WHAT THIS DOES FOR YOU

The good news

Every one of these problems is easy to prevent. A written list, a shared phone passcode, and a few free settings at Apple, Google and your password manager take care of most of it. That's what Part 2 and Part 3 of this guide are for.

FROM BILL

If you're here after a loss

If you're reading this because someone has already died and nothing was planned, please don't lose heart. There are still good options, and Part 5 and Part 6 walk you through them. Start with Chapter 15, which covers what to do first and, just as important, what can wait.

PART 2

Taking Stock

Make a simple list of what you have, make sure someone can get past the locks that matter most, and keep it all somewhere safe.

CHAPTER 4

Making Your Digital Inventory

The single most useful thing you can do for your family is make a list. Not a list of every website you've ever visited, just the accounts and devices that matter. Think of it as a map for whoever comes after you.

WHAT THIS DOES FOR YOU

What this does for you

An executor or family member with a good list can handle in an afternoon what might otherwise take months of detective work: finding which bank you used, which subscriptions to stop, and where the photos live.

What to write down

For each account, note these few things. You don't need fancy software; a notebook works fine.

Write down	For example
What it is	"Gmail," "Chase checking," "Netflix," "Facebook"
The website or app	So nobody has to guess which company it is
The sign-in name	Usually your email address or a username
Where the password is	"In my password manager," or "in the sealed envelope" (see Chapter 7)
Does it cost money?	Monthly or yearly, and which card pays it
What you'd like done	Close it, keep it, memorialize it, or pass it to someone

Start with the big ones

1. Your **phones, tablets and computers**, and how each one unlocks.
2. Your main **email account**. This is the master key, because password resets go there.
3. Your **Apple Account** or **Google Account** (or both). These hold photos, contacts and backups.
4. Your **bank, credit card, investment and retirement** accounts that you use online.
5. Anything that **charges you automatically**: streaming, cloud storage, Amazon Prime, apps, magazines.
6. **Social media** accounts and what you'd like done with them.

7. Utilities and services you pay online: electric, gas, water, internet, phone.

A quick way to find the subscriptions

Look through two or three months of credit card and bank statements and circle anything that repeats. On an iPhone, you can also open **Settings**, tap your name, then tap **Subscriptions** to see what you pay for through Apple. On an Android phone, open the **Google Play Store**, tap your profile picture, then **Payments & subscriptions**.

TIP

Don't let it become a chore

You don't have to finish in one sitting. Do the phone, email and bank today, and add the rest a few at a time. A list that's 80 percent done is far more useful than a perfect one you never start.

STAY SAFE

Guard the list like cash

A list with passwords on it is valuable to a thief. If you write passwords down, keep that page somewhere secure (Chapter 7 has good options), and never email it or keep it as an unprotected file on the computer.

CHAPTER 5

The Keys That Matter Most

Of everything on your list, three "keys" open the most doors: your **phone passcode**, your **computer password**, and your **main email**. If your family has these, almost everything else can be found or reset.

Your phone passcode

Your phone is probably where your most recent photos and messages live, and it's often the device that receives sign-in codes for everything else. Modern phones are encrypted, so without the passcode the phone can't be opened. Apple says it can't remove a passcode lock without erasing the device, which would erase whatever wasn't backed up.

So please make sure at least one trusted person knows your phone passcode, or that it's written in your sealed envelope or password manager. If you change it, update the note.

GOOD TO KNOW

Face ID and fingerprints won't be enough

Phones regularly ask for the passcode itself, for example after a restart, even if you normally unlock with your face or fingerprint. A family member needs the actual numbers.

Your computer password

Write down how your computer signs in: a password, a PIN, or the password of a Microsoft or Apple account. On many Windows computers the sign-in is your Microsoft account; on a Mac it's the user password you chose when you set it up.

Your main email

Email is the master key because nearly every company sends its "reset your password" link there. Whoever can read your email can usually reset the rest. That's exactly why you want to protect it carefully now, and exactly why your executor will need it later.

WHAT THIS DOES FOR YOU

What this does for your family

With these three keys, a family member can save the photos on your phone, turn off subscriptions, download statements and close accounts properly, rather than fighting each company one at a time.

CHAPTER 6

Two-Factor Sign-In and the Phone Number Problem

Two-factor sign-in (also called two-step verification) means that after you type your password, the company also asks for a second proof, usually a short code sent by text message or shown in an app. It's one of the best protections you can have, and I recommend it. But it has a side effect your family needs to know about.

Why the phone number matters so much

If your accounts send their codes to your cell phone number, then whoever needs to sign in later needs that phone, or at least that phone number. If the family cancels the phone line too soon, those codes stop arriving, and accounts can become very hard to get into.

HEADS UP

Don't cancel the phone line first

After a death, keep the person's phone line active, even on a cheaper plan, until you've finished with their accounts. It's often the only way to receive the sign-in codes. Chapter 17 covers this in more detail.

Planning ahead for two-factor

- Write down **which phone number** your accounts use for codes.
- If you use an **authenticator app** (such as Google Authenticator or Microsoft Authenticator), note that it lives on your phone, so the phone passcode matters even more.
- Many accounts give you **backup codes** or **recovery codes** when you turn on two-factor. Print them and keep them with your important papers.
- Some accounts let you add a **recovery phone or email** belonging to a trusted family member. That can help both you and them if you're ever locked out.

SCAM ALERT

Codes are never for strangers

A sign-in code is the last lock on the door. Never read one aloud to someone who calls, texts or emails you, even if they say they're from your bank, Apple, Amazon or the government. Real companies don't ask. That rule matters even more for a grieving family, as Chapter 23 explains.

CHAPTER 7

Where to Keep It All Safely

Now that you have a list, where should it live? The goal is a place that's safe from thieves while you're alive, and easy for the right person to find when the time comes. Here are the honest options.

Option	Good for	Watch out for
A **password manager** with emergency access (Chapter 12)	Passwords that change; it stays up to date	Someone still needs to know how to get in
A **sealed envelope** with your will or in a home safe	Phone passcode, master password, recovery codes	Must be updated when passwords change
A **safe deposit box**	Very secure storage of the paper list	Family may need legal paperwork to open it
Your **estate attorney**	Keeping your written wishes with your will	Don't put passwords in the will itself; wills can become public records

My suggestion for most families

1. Use a **password manager** for everyday passwords, and set up its **emergency access** for a trusted person.
2. Put the few things that unlock everything else (phone passcode, computer password, password manager master password, and any recovery codes) in a **sealed envelope**.
3. Tell your executor or a trusted family member **where the envelope is**.
4. Set up **Apple's Legacy Contact** and **Google's Inactive Account Manager** (Chapters 8 and 9). These work even if the envelope goes missing.
5. Look at the envelope once a year, perhaps on your birthday, and update anything that's changed.

GOOD TO KNOW

Ohio has a law about digital accounts

Ohio has adopted the **Uniform Fiduciary Access to Digital Assets Act**, found in the Ohio Revised Code (ORC 2137). It sets out when an executor or other fiduciary can reach a person's online accounts and how the person's own instructions are honored. What it means for your situation is a question for your estate attorney. Mention your digital accounts when you meet with them.

FROM BILL

A note on wills

Please don't write passwords into your will. A will may be read by many people and can become part of the public court record. Instead, the will (or a letter kept with it) can say *where* your list and envelope are, and who you'd like to handle your digital accounts.

PART 3

Setting It Up, Company by Company

The free planning tools from Apple, Google and Facebook, what to do for companies that don't offer one, and how password managers let a trusted person in.

CHAPTER 8

Apple: Adding a Legacy Contact

If you have an iPhone, iPad or Mac, this is the most important setting in this guide. A **Legacy Contact** is someone you choose who can ask Apple for access to the data in your Apple Account after your death. Apple calls it the easiest, most secure way to do this.

WHAT THIS DOES FOR YOU

What this does for you

Without a Legacy Contact, Apple generally needs a court order before it will let family into your account. With one, your chosen person needs only two things: the **access key** Apple creates for them, and a **death certificate**.

What your Legacy Contact can and can't see

They can access	They can't access
iCloud Photos, Notes, Mail, Contacts, Calendars, Reminders	Movies, music and books you bought
Messages in iCloud and call history	Subscriptions and in-app purchases
Files in iCloud Drive, Health data, Voice Memos	Payment information for Apple Account or Apple Pay
Safari bookmarks, and anything in an iCloud Backup	Passwords and passkeys stored in iCloud Keychain

GOOD TO KNOW

Passwords aren't passed on this way

Notice that saved passwords are *not* included. That's why Chapter 12, on password managers, matters too. Apple's Legacy Contact is for photos, messages and files; your passwords need their own plan.

Before you start

- Your device needs iOS 15.2, iPadOS 15.2 or macOS Monterey 12.1 or later. Any current iPhone qualifies.
- You need to be signed in to your Apple Account, with **two-factor authentication** turned on.
- Your Legacy Contact does **not** need an Apple device or an Apple Account.

- They must be over 13 to make a request (the age varies by country).

To add a Legacy Contact on iPhone or iPad

1. Open **Settings** and tap **your name** at the top.
2. Tap **Sign-In & Security**, then tap **Legacy Contact**.
3. Tap **Add Legacy Contact**. You may need to use Face ID, Touch ID or your passcode.
4. Choose someone from your Family Sharing group, or tap **Choose Someone Else** to pick from your contacts.
5. Choose how to share the access key: **Send an iMessage** (their device saves the key automatically when they accept) or **Print a Copy** (to hand them, or keep with your estate papers).

On a Mac, it's the same idea: Apple menu > **System Settings**, click your name, then **Sign-In & Security** > **Legacy Contact**. Apple emails you a confirmation when a contact is added.

The access key is precious

Apple can't look up or replace an access key that's been lost. If you sent it by iMessage, check that your contact actually received it. Either way, Apple suggests also printing a copy for your estate planning documents. To see it again later: **Settings** > your name > **Sign-In & Security** > **Legacy Contact**, tap the person's name, then tap **View Access Key**.

HEADS UP

More than one Legacy Contact

You can add several, which is a good idea in case one isn't available. But know this: any one of them can make decisions about your data on their own, including permanently deleting it. Choose people who will work together.

TIP

Access lasts three years

Once Apple approves a request, the Legacy Contact can use the account for three years, and then it's permanently deleted. Tell your contacts to download anything they want to keep, especially photos.

CHAPTER 9

Google: The Inactive Account Manager

If you use Gmail, Google Photos or an Android phone, Google offers a similar planning tool called the **Inactive Account Manager**. It works a little differently from Apple's: instead of waiting for a death certificate, it acts when your Google Account has gone unused for a length of time you choose.

WHAT THIS DOES FOR YOU

What this does for you

You decide, in advance, who should receive your photos, email or files, and Google sends them a download link automatically if your account goes quiet. No court order, no paperwork, no arguing with a help line.

How it works

- You choose **how long** Google should wait after your account stops being used.
- You pick **up to 10 people** to notify, and choose whether each one gets all of your data or only certain kinds, such as Photos or Drive.
- Google asks for each person's **phone number**, so it can make sure only that person downloads your data.
- Your contacts hear **nothing** while you're setting it up. They're only contacted once your account has been inactive for the time you chose.
- You can write the email they'll receive. Google adds a short note explaining that you asked it to send the message.

To set it up

1. On a computer or phone, go to **myaccount.google.com/inactive** and sign in to your Google Account.
2. Choose how long Google should wait before acting.
3. Add the people you'd like Google to contact, with their email and phone number, and choose what to share with each.
4. Optionally, write the subject and message they'll receive.
5. Review your plan and save it.

GOOD TO KNOW

How Google knows you're still around

Google looks at signals like your recent sign-ins, your activity in Google's services, use of Gmail (including the Gmail app on your phone) and check-ins from your Android phone. Ordinary everyday use keeps your plan from starting.

HEADS UP

If you don't set a plan

Google says it may delete an account that's been inactive across Google for at least two years. Without a plan, your family would have to ask Google for help after the fact, and Google only provides a deceased person's content "in certain circumstances." Setting a plan now is far more certain.

TIP

Change it any time

You can return to the same page to change your contacts, choose different data, or turn the plan off altogether. It's worth a quick look once a year when you review your envelope.

CHAPTER 10

Facebook & Instagram: Memorial or Goodbye

Social media is more personal than most accounts. Some families find great comfort in a memorial page where friends share stories and photos; others prefer the account simply be taken down. Facebook lets you decide ahead of time.

Your two choices on Facebook

Choice	What it means
Memorialize it	Your profile stays up with the word "Remembering" next to your name, so friends can share memories. You can name a **legacy contact** to look after it.
Delete it	You can ask Facebook to permanently delete your account after you've passed away.

What a legacy contact can do

A Facebook **legacy contact** is someone you choose to look after your memorialized profile. Facebook says they can't read your messages, log into your account or remove your friends. Their role is to care for the memorial: for example, pinning a post with service details and updating the profile and cover pictures.

To set your choice

1. Open Facebook and go to **Settings & privacy**, then **Settings**.
2. Open **Accounts Center**, and look for the **Memorialization** setting (it sits with the account ownership and control options).
3. Choose a legacy contact from your friends, or choose to have your account deleted after you pass away.
4. Save your choice.

TIP

Tell your legacy contact

Facebook doesn't tell the person when you choose them. It only lets them know once your account has been memorialized. Have a quiet word with them now, so it doesn't come as a surprise.

GOOD TO KNOW

Facebook moves its menus around

Meta has rearranged these settings more than once. If your screen looks different, use the search box in Settings and type **memorialization** or **legacy contact**.

Instagram

Instagram doesn't let you name a legacy contact the way Facebook does. After a death, a family member can ask Instagram to memorialize the account or, as an immediate family member, ask for it to be removed. Chapter 20 covers how. For now, simply write your wishes on your list.

CHAPTER 11

Microsoft, Amazon & Accounts Without a Tool

Many companies don't offer a planning tool at all. For these, your list and your sealed envelope do the work, and it helps to understand each company's rules now.

Microsoft (Outlook.com, Hotmail, OneDrive, Microsoft 365)

Microsoft is clear and strict. If the family has the sign-in details, they can close the account themselves. If not, Microsoft won't release email or OneDrive files to family members without a valid subpoena or court order, and even then makes no promises. Outlook.com and OneDrive accounts are frozen after one year without use, with email and files deleted shortly after.

TIP

So, for Microsoft accounts

Put the Microsoft account email and password in your password manager or envelope. And keep a copy of your most precious OneDrive photos and documents somewhere else too, such as a USB drive or a family member's cloud account (Chapter 13).

Amazon

I couldn't confirm any plan-ahead tool at Amazon. Put the Amazon sign-in in your list, and note whether you have Prime, Kindle Unlimited, Audible or other memberships that bill automatically. After a death, the family will need to contact Amazon customer service directly.

Banks and investment accounts

Banks follow their own legal procedures after a death, usually involving the executor and a death certificate. You don't need to give anyone your banking password for that. What helps most is simply listing *which* banks and brokerages you use, so nothing is overlooked. Ask your bank about payable-on-death or beneficiary designations; your attorney can explain how they fit your plan.

Smaller accounts

Streaming services, shopping sites, newspapers and apps mostly stop on their own once the credit card they bill is closed or the family cancels them. Just make sure they're on the list with "costs money" marked, so someone remembers to check.

GOOD TO KNOW

Cryptocurrency, briefly

If you own any cryptocurrency, please treat it with extra care. Coins held on an exchange (such as Coinbase) are generally handled through that company's estate process. Coins held in your own "wallet" may be impossible for anyone to recover without the wallet's recovery phrase. Tell your attorney you own it, and keep the recovery phrase on paper somewhere secure, never in an email or photo.

CHAPTER 12

Password Managers: Emergency Access

A **password manager** is an app that remembers all your passwords for you, locked behind one master password. (If you don't use one yet, our Passwords & Password Managers guide explains them gently.) The good ones also give you a way to let a trusted person in during an emergency.

WHAT THIS DOES FOR YOU

What this does for you

Instead of a sealed envelope full of passwords that go out of date, your family gets the live, up-to-date list, exactly as you kept it, through the password manager's own safe process.

Bitwarden: Emergency Access

Bitwarden has a feature called **Emergency access**. You name a trusted person and choose a waiting period. If they ever request access and you don't say no within that time, they're let in. Adding a trusted contact needs a paid Bitwarden plan (Premium, or a paid Families plan); the person you choose only needs a free Bitwarden account.

1. In the Bitwarden **web app** (on a computer, at bitwarden.com), go to **Settings** > **Emergency access**.
2. Select **+ Add emergency contact** and enter the person's email.
3. Choose their access: **View** (they can see your passwords) or **Takeover** (they can take over the account).
4. Set the **Wait time**. The shortest allowed is one day.
5. Select **Save**. They must accept the emailed invitation within five days.
6. After they accept, go back to **Emergency access**, open the menu next to their name and select **Confirm**, checking the fingerprint phrase with them.

GOOD TO KNOW

If you stop paying

Bitwarden says that if your premium plan lapses, contacts you've already set up can still request and get access. You just can't add new ones or change them.

1Password: the Emergency Kit

1Password's planning tool is a one-page **Emergency Kit**, a PDF with your sign-in address, email and **Secret Key**, plus a space to write your account password. 1Password suggests printing it, keeping it in a safe deposit box or with your passport or birth certificate, and giving a copy to someone you trust, like your spouse or someone named in your will.

1. Sign in to your account at **1Password.com**.
2. Select your name in the top right, then **Manage Account**.
3. Select **Save Emergency Kit** and save the PDF.
4. Print it, write your account password on at least one copy, and put it with your important papers.

Apple's Passwords app: shared groups

If your passwords live in Apple's **Passwords** app, you can create a **shared group** and invite a trusted family member. Everyone in the group can see and use the passwords you put in it. Only the person who created the group can add or remove people. This works on iOS 17, iPadOS 17 and macOS Sonoma or later, and the people you add need to be in your contacts.

HEADS UP

Sharing is immediate

Unlike Bitwarden's waiting period, a shared group shares the passwords *right away*, while you're alive. Use it only with someone you'd trust with your wallet, and share only what they truly need, such as the household utilities and streaming services. Apple notes that removing someone later doesn't undo what they've already seen, so you'd want to change those passwords.

FROM BILL

Whichever you use

Your password manager's own master password is the one password that can't live inside it. Make sure it's in your sealed envelope, or that your emergency access is set up, or both.

PART 4

Photos, Memories & Your Wishes

Make sure the pictures survive no matter what, and put your wishes in writing so your family doesn't have to guess.

CHAPTER 13

Making Sure the Photos Survive

When families talk about what they want most after a loss, it's almost always the photos and videos. The good news is that protecting them is easier than protecting almost anything else. The idea is simple: photos that exist in more than one place are photos that won't be lost.

WHAT THIS DOES FOR YOU

What this does for you

If your photos are backed up to the cloud and copied somewhere your family can reach, they're safe even if your phone is lost, broken, or locked with a passcode nobody knows.

Step one: make sure the phone is backing up

On an iPhone, check that **iCloud Photos** is on: open **Settings**, tap your name, tap **iCloud**, then **Photos**, and make sure **Sync this iPhone** is turned on. On an Android phone, open the **Google Photos** app, tap your profile picture, and check that backup is on. (Our Backing Up Everything and iCloud guides cover these settings step by step, including storage plans.)

HEADS UP

Free storage fills up

Apple gives 5 GB of iCloud storage free and Google gives 15 GB shared across Gmail, Drive and Photos. Many people fill that up without noticing, and backups quietly stop. If your phone keeps nagging that storage is full, that's your sign to deal with it.

Step two: keep a copy your family can reach

Pick one or two of these. Each puts a copy of your photos outside your own locked account:

- **A shared album** with your children or grandchildren, for the photos that matter most.
- **Family Sharing** (Apple) or a shared family storage plan, so a trusted person already has access to the account's storage.
- **A USB drive or external hard drive**, copied once or twice a year and kept with your important papers.
- **Your Legacy Contact or Inactive Account Manager plan** (Chapters 8 and 9), which hands over the whole library later.

Google Takeout: a full copy of your Google data

Google lets anyone download a complete copy of their own data, photos included, using a service called **Google Takeout**. Downloading a copy doesn't delete anything from Google.

1. On a computer, go to **takeout.google.com** and sign in.
2. The products you use are already checked. Uncheck any you don't want. To save only photos, leave just **Google Photos** checked.
3. Select **Next step**.
4. Under **Delivery method**, choose **Send download link via email** (or have it added to Google Drive, Dropbox, OneDrive or Box).
5. Select **Create export**. When the email arrives, select **Download archive**.

TIP

Set it and forget it

Takeout can also make **scheduled exports** automatically every two months for a year. For Google Photos, you can schedule exports of new and updated photos, as long as Photos is the only product selected. Note that each download link expires after about a week, so download it promptly.

Photos on a computer or old memory cards

Don't forget the pictures that never made it to a phone: folders on an old computer, CDs from the drugstore, camera memory cards in a drawer. Gather them onto one drive and label it clearly, "Family photos, copy for the kids." Our Digitizing Old Photos & Movies guide covers prints and slides.

CHAPTER 14

Writing Down Your Wishes

Passwords open doors. But your family also needs to know which doors you'd like opened, and what to do once they're inside. A short letter of wishes, kept with your list, answers the questions they'll otherwise have to guess at.

WHAT THIS DOES FOR YOU

What this does for your family

When wishes are written down, there's less to decide and less to disagree about during a hard time. Family members can simply say, "This is what Mom wanted."

Questions worth answering

- Who should handle your digital accounts? (Often the same person as your executor, but it doesn't have to be.)
- Should your Facebook page be **memorialized** or **deleted**? Any other social accounts?
- Is there anything private you'd like **deleted unread**: a journal, certain emails, a folder?
- Who should get your **phone, tablet and computer**, or should they be wiped and recycled?
- Which photos or videos would you most like shared with the whole family?
- Are there online friends, clubs or groups who should be told, and how?
- Any accounts that should be kept open for a while, such as an email address many people know?

Where to keep the letter

Keep it with your digital inventory (Chapter 4) and tell your executor where both are. Your estate attorney can keep a copy with your will. A letter of wishes like this usually doesn't contain passwords, so it's fine to give copies to the family members it concerns.

GOOD TO KNOW

A conversation is a gift too

If you can, talk it through with the person who'll handle things. Showing them where the envelope is, and how your Legacy Contact access key works, takes ten minutes and spares them a great deal of worry later.

A yearly check-up

1. Pick a date you'll remember, such as your birthday or New Year's Day.
2. Update your inventory: new accounts, closed accounts, new subscriptions.
3. Update any passwords or passcodes in the envelope that have changed.
4. Make sure your Apple Legacy Contacts and Google Inactive Account Manager contacts are still the right people.
5. Copy any new photos to your USB drive or shared album.

PART 5

When Someone Has Died

For families after a loss: what to do in the first days, how to protect your loved one's identity, and how to stop the mail, the phone bill and the subscriptions in the right order.

CHAPTER 15

The First Days: What to Do and What Can Wait

I'm so sorry for your loss. If you're reading this soon after a death, please know that almost nothing digital is urgent. The accounts will still be there next week. Take care of yourself and your family first, and come back to this when you're ready.

The few things worth doing early

1. **Keep their phone charged and safe.** Don't reset it or let a well-meaning relative "clean it up." It may hold photos that exist nowhere else, and it receives sign-in codes.
2. **Keep their phone line active.** Don't cancel it yet (Chapter 17 explains why).
3. **Gather their devices**: phone, tablet, computer, and any papers with passwords or a Legacy Contact access key.
4. **Look for their plan.** Check for a digital inventory, sealed envelope or letter of wishes, and ask the executor or attorney whether one was left with the will.
5. **Order several certified copies of the death certificate.** Nearly every company will ask for one. The funeral home can usually help with this.

Things that can wait

- Closing email and social media accounts.
- Deciding what to do with their computer and phone.
- Sorting through photos and files.
- Canceling small subscriptions (a few extra dollars is not worth stress right now).

FROM BILL

Go gently

There's no prize for finishing quickly. Many families find it easier to sit down together, a few weeks on, and go through the phone and photos as a way of remembering. If you'd like a patient person there to handle the technical side, that's what I'm here for.

Social Security

Funeral homes generally report a death to Social Security, so families usually don't need to. If no funeral home was involved, or it didn't report the death, call Social Security at **1-800-772-1213** (TTY 1-800-325-0778), Monday through Friday, 8 a.m. to 7 p.m. Have the person's name, Social Security number, date of birth and date of death ready.

GOOD TO KNOW

A small payment some families can receive

Social Security says a surviving spouse might get a one-time death payment of $255, and some children may be eligible if there's no spouse. Certain family members may also qualify for monthly survivor benefits. Ask when you call, or see ssa.gov.

CHAPTER 16

Protecting Their Identity

It's a hard thing to hear, but identity thieves sometimes target people who have recently died, because nobody is watching their credit. A few calm steps make that very unlikely.

WHAT THIS DOES FOR YOU

What this does for your family

These steps stop a stranger from opening credit cards or loans in your loved one's name, which could otherwise cause a mess for the estate and for you.

The steps

1. **Make sure Social Security has been told** (Chapter 15). Funeral homes usually do this.
2. **Contact each of the three credit bureaus**, Equifax, Experian and TransUnion, tell them about the death and ask how to protect the credit file. Each has its own process, and you'll usually need a copy of the death certificate and proof that you're the spouse or executor.
3. **Watch the mail and the bank statements** for anything unexpected: new cards, bills, or collection letters.
4. **Keep personal details out of the obituary**, such as the exact birth date and home address (Chapter 24).
5. **Shred**, don't toss, old statements and papers with their Social Security number.

GOOD TO KNOW

What a credit freeze is

A **credit freeze** keeps people from getting into a credit report, so nobody can open a new credit account. The FTC notes that freezes are free and that you contact *each* of the three bureaus to place one.

If you think someone has already misused their identity

Report it to the Federal Trade Commission at **IdentityTheft.gov**. You'll get a personal recovery plan and pre-filled letters to send to credit bureaus and businesses. You can also call **877-438-4338**.

SCAM ALERT

Nobody official will call asking for the Social Security number

The FTC says organizations like the IRS and your bank won't call, email or text to ask for a Social Security number. If someone calls "about the estate" and asks for it, it's a scammer. Hang up and call the organization back at a number you look up yourself.

CHAPTER 17

Mail, the Phone Line & Subscriptions

The order you do things in matters here. Close the wrong thing first and you can lock yourself out of everything else. Here's the order I suggest.

1. Keep the phone line on, for now

Many accounts send sign-in codes to the person's cell phone number by text. If the line is canceled, those codes stop, and getting into accounts gets much harder. Call the phone company, explain the situation, and ask about keeping the number active on the cheapest plan for a few months. When you're finished with the accounts, you can cancel it, or ask the carrier whether a family member can take over the number.

> **TIP**
> **Sign-in codes can come to the phone even when it's locked**
> On many phones, a text with a code shows up on the lock screen. If you have the phone but not the passcode, you may still be able to read codes as they arrive, which can help you sign in to an account when you have the password.

2. Save what you need from their email

Before closing anything, look through their email (if you can get in) for statements, bills, subscription receipts and online accounts you didn't know about. Searching their inbox for words like **receipt**, **subscription**, **renewal** and **statement** is a quick way to build the list they may not have left you.

3. Stop the subscriptions

- **Apple subscriptions:** on their iPhone, **Settings** > their name > **Subscriptions**.
- **Google Play subscriptions:** in the Play Store, profile picture > **Payments & subscriptions**.
- **Amazon Prime and other services:** sign in to each website and cancel, or call customer service.
- **Anything you can't get into:** the charges stop when the card or bank account they bill is closed. Microsoft, for example, says subscriptions can be stopped by closing the card or bank account or telling the bank.

4. Mail

Paper mail is often how you discover accounts you didn't know about, so don't stop it too soon. The executor can contact the local post office about having the person's mail sent to them. Watch it for a few months for statements, renewals and anything unexpected.

5. Close the card and bank accounts last

Let the executor handle bank and credit card accounts with the bank directly. Closing the main card is often what finally stops the small subscriptions nobody found, so it makes sense to do it after you've saved the statements you need.

HEADS UP

Don't use their accounts to pay for things

It can be tempting to keep using a loved one's card or account "just to finish things up." Let the executor and the bank guide what's allowed. That's a legal question, and your estate attorney is the right person to ask.

PART 6

Their Accounts & Devices

Company by company: how to reach, keep or close a loved one's Apple, Google, Facebook, Microsoft and Amazon accounts, save their photos, and decide what to do with their devices.

CHAPTER 18

Their Apple Account

What you can do with a loved one's Apple Account depends on one question: **did they name you as a Legacy Contact?** If they did, the path is fairly simple. If not, there are still options, but they need more paperwork.

If you're their Legacy Contact

You'll need two things: the **access key** and a **death certificate**. The key may already be saved on your own iPhone, or it may be printed, emailed, or tucked in with their estate papers. Apple says the scanned death certificate should be flat, fully legible, with all four edges visible, in PDF, PNG, TIF, JPEG or GIF format.

To request access from your iPhone or iPad

1. Open **Settings** and tap **your name**.
2. Tap **Sign-In & Security**, then tap **Legacy Contact**.
3. Tap your loved one's name.
4. Tap **Request Access** and follow the steps to upload the death certificate.

Or on the web, if you don't have an Apple device

1. Go to Apple's Digital Legacy website, **digital-legacy.apple.com**.
2. Click **Request access**.
3. Sign in with your own Apple Account, or choose the option for people who don't have one.
4. Follow the steps to verify your identity, enter the access key, and upload the death certificate.

What happens next

- Apple emails you to confirm it received the request, and reviews it. You can check the status on the Digital Legacy website.
- Once approved, you'll get a special **Legacy Contact Apple Account**. You'll enter the access key again, create a password and set up two-factor authentication for it.
- Your loved one's original Apple Account stops working, and **Activation Lock** is removed from their devices.

- You can sign in at **iCloud.com** to view and download their photos and files, and get a copy of their data at **privacy.apple.com**. You can also restore their iCloud Backup to an iPhone or iPad.
- Access lasts **three years** from approval, then the account is permanently deleted.

HEADS UP

Download the photos early

Don't let the three years slip by. Download the photos and anything else you want to keep within the first few months, and make a second copy for another family member.

If there's no Legacy Contact

Apple can still help, but it needs legal documents. In the U.S., you can ask for access with a **court order** that names you as the rightful inheritor of your loved one's personal information. Only one person can request access this way. Some data is end-to-end encrypted and Apple can't decrypt it. Your estate attorney can explain how to get such an order. Or, if you only want the account **closed**, Apple's Digital Legacy website has a separate request to permanently delete a deceased person's account; you'll need an Apple Account of your own and the required documents.

CHAPTER 19

Their Google Account

Google gives families two routes: the plan your loved one may have set up themselves, and a request you can make to Google after the fact.

If they set up the Inactive Account Manager

If your loved one used the Inactive Account Manager (Chapter 9), you may receive an email from Google once their account has been inactive for the time they chose. It will list the data they shared with you and give you a link to download it. Google will ask you to verify your phone number, so only you can download it.

> TIP
> **Watch your email, including the spam folder**
> Because the email comes from Google automatically, weeks or months after the death, it's easy to miss. Tell the family to watch for it, and download the data as soon as it arrives.

If they didn't, ask Google

Google says it can work with immediate family members and representatives to close a deceased person's account where appropriate, and in certain circumstances may provide content from it. Requests go through Google's **deceased user** request form in Google Account Help. You'll be asked for details about yourself and the person, and for a death certificate.

> HEADS UP
> **Get the data before you close it**
> If you'd like to keep photos or email, ask for the content first. Closing the account is final.

If you have their password

If the family has the sign-in details and the phone that receives the codes, the simplest way to save their photos and email is **Google Takeout**, exactly as described in Chapter 13. Download everything you want before deciding whether to close the account.

GOOD TO KNOW

Google may delete idle accounts

Remember, Google says it may delete an account that's been inactive across Google for two years. Don't wait indefinitely to save what matters.

CHAPTER 20

Facebook, Instagram, Microsoft, Amazon & the Rest

Each company has its own rules. Here's what to expect from the ones families ask about most.

Facebook

If your loved one named a **legacy contact**, that person can look after the memorialized profile (Chapter 10). If they didn't, a family member or friend can ask Facebook to **memorialize** the account, and immediate family or the executor can ask for it to be **removed**. Search Facebook's Help Center for "memorialization request" or "deceased person's account" to find the current forms. You'll typically be asked for the person's name, date of death, and a link to the profile or proof of death, such as an obituary.

> GOOD TO KNOW
> **Memorialized means locked**
> Once an account is memorialized, nobody can log into it, and the content stays as it was. If there's no legacy contact, the profile generally can't be changed afterward. Decide as a family before you ask.

Instagram

Instagram, also owned by Meta, has its own forms for memorializing an account or, for immediate family, removing it. Search the Instagram Help Center for "deceased."

Microsoft (Outlook.com, Hotmail, OneDrive)

- You **don't need to tell Microsoft** that someone has died.
- **If you know the sign-in**, you can close the account yourself. Microsoft keeps it for 60 days in case you change your mind, then deletes it permanently. Save anything you want first.
- **If you don't**, cancel any Microsoft subscriptions through the bank or card. Microsoft will only consider releasing email or files after being served with a valid subpoena or court order, and makes no guarantees.

- Outlook.com and OneDrive are frozen after a year without use, and the account expires after two years.

Amazon

If you have the sign-in, you can cancel Prime and other memberships yourself in the account settings. Otherwise, contact Amazon customer service, explain that the account holder has died, and ask what they need. Have the death certificate and proof that you're the executor ready.

Everything else

Type of account	What usually works
Streaming (Netflix, Hulu and so on)	Sign in and cancel, or let it end when the card is closed
Email from the internet provider (Spectrum, AT&T, etc.)	Call the provider; ask about saving mail before the service ends
Online banking and investments	The executor works with each bank directly
Smaller social sites and forums	Look for a help page about deceased members, or simply leave it
Rewards and airline miles	Ask the company; rules vary a great deal

CHAPTER 21

Saving the Photos From Their Phone & Computer

For many families this is the part that matters most. Take your time, and don't erase or reset anything until you're sure the photos are safely copied in at least two places.

If you know the phone's passcode

1. Charge the phone and connect it to Wi-Fi.
2. Check whether the photos are already in the cloud: on an iPhone, **Settings** > their name > **iCloud** > **Photos**; on Android, open **Google Photos** and look for the backup status under their profile picture.
3. If they're backed up, you can download them later from iCloud.com or Google Takeout (Chapters 18 and 19).
4. If they're *not*, copy them now. Connect the phone to a computer with its charging cable and import the photos, or share the most important albums to your own phone.
5. Copy the result to a USB drive as well, so there are two copies.

If you don't know the passcode

This is the hard case. Apple says it can't remove a passcode lock without erasing the device, and Android phones are protected the same way. So don't guess endlessly: too many wrong tries can lock the phone for longer and longer periods, and some phones are set to erase themselves after too many failures.

Instead, look for the photos in the cloud. If your loved one used iCloud Photos, a Legacy Contact or a court order can get you to them (Chapter 18). If they used Google Photos, their Inactive Account Manager plan or a request to Google may (Chapter 19). Also look at other family members' phones: many photos were probably shared in texts and albums over the years.

SCAM ALERT

Beware "we can unlock any phone" services

Websites and shops that promise to unlock any locked phone for a fee are, at best, unreliable and, at worst, a scam. Some ask you to mail the phone away. Please talk to someone you trust before you hand over a loved one's phone or pay anyone to "crack" it.

Their computer

Photos on a computer are usually in the **Pictures** folder (Windows) or the **Photos** app (Mac). If you can sign in, copy that folder to a USB drive. Also check the desktop and the Downloads and Documents folders, and any external drives or memory cards lying nearby.

CHAPTER 22

Their Devices: Keep, Pass On or Wipe

Once the photos and files are safe, you can decide what to do with the phone, tablet and computer. Whatever you choose, a device should be properly **erased** before it leaves the family.

Apple devices and Activation Lock

iPhones, iPads and Macs have **Activation Lock**, which ties them to the owner's Apple Account so a thief can't use them. After a Legacy Contact request or an account deletion request is completed, Apple removes Activation Lock automatically. The device then needs to be erased and restored before someone else can use it with their own Apple Account.

Before you erase any device

1. Make sure the photos, videos and documents you want are copied in **two places** (Chapter 21).
2. Write down anything useful from it, such as contacts you may need to notify.
3. If you can, **sign out** of their Apple Account or Google Account on the device first.
4. Remove any SIM card and memory card, and keep them with the estate papers.
5. Then erase it. On an iPhone, that's **Settings** > **General** > **Transfer or Reset iPhone** > **Erase All Content and Settings**. On Android, open **Settings** and search for **reset** to find the factory reset option.

HEADS UP

Android phones remember their Google Account

After a reset, an Android phone may ask for the Google Account that was last signed in. Removing the account from **Settings** before you reset avoids that. If you can't, the phone may not be usable by someone else.

Computers

Windows and Mac computers both have a built-in reset that erases everything and reinstalls the system. If the computer is old and simply going to recycling, many recyclers will destroy the drive for you; ask before you drop it off. Our Windows 11 and Mac guides show the reset steps.

WHAT THIS DOES FOR YOU

Passing a device on, with care

A grandchild may treasure Grandpa's iPad. Once it's erased, it's as good as new to them, and the family photos can be loaded back on from the copy you saved.

PART 7

Staying Safe in a Hard Time

Scammers watch for grieving families. Here's how their tricks work, and how to write an obituary that honors your loved one without helping a thief.

CHAPTER 23

Scams That Target Grieving Families

It's a cruel truth that some criminals look for families who have just lost someone. They count on you being tired, distracted and eager to settle things. Knowing their few tricks takes away their power.

The tricks to know

The trick	What it looks like
"Your loved one owed us money"	A caller or letter demands payment of a debt you've never heard of, often with a threat. Real debts are handled through the estate; ask for it in writing and show it to the executor or attorney.
Fake government calls	Someone claims to be from Social Security, Medicare or the IRS and needs a Social Security number, a payment, or a gift card "to settle the account."
Tech support pop-ups	While you're on their computer, a pop-up says it's infected and to call a number. It's never real. Close it and call someone you trust.
"Unlock the phone" or "recover the account" services	Promises to get into a loved one's phone or Facebook for a fee. Real access comes only through the company itself.
Messages from the deceased's hacked account	Friends get messages from your loved one's account asking for money. Tell friends and family not to respond, and report the account to the company.
Funeral or flower payment scams	Fake requests to pay for services, sent to friends by email or text.

SCAM ALERT

Gift cards are a giveaway

No real company, agency or funeral home asks to be paid in gift cards, wire transfers or cryptocurrency. The moment someone asks for one of those, you know it's a scam.

SCAM ALERT

Never share a sign-in code

If someone calls offering to "help close the account" and asks you to read back a code that was just sent to your loved one's phone, hang up. That code is the key to the account.

Three habits that stop almost every scam

1. **Slow down.** Anyone who says it must be done today is a warning sign.
2. **Call back on a number you look up yourself**, from a statement, the company's real website or the back of a card.
3. **Check with someone** before you pay, share a number, or let anyone onto a computer: the executor, a family member, or me.

If you've already paid or shared something, don't be embarrassed. Report it at **ReportFraud.ftc.gov**, call the bank, and see Chapter 16 for protecting the person's identity. Our Spotting & Avoiding Scams guide goes into much more detail.

CHAPTER 24

An Obituary That Doesn't Help Thieves

An obituary is a loving tribute, and it should be. But identity thieves read them too, looking for the details that unlock accounts and credit. A few small choices keep your family safe without taking anything away from the tribute.

Consider leaving out

- The **exact date of birth**. The age, or just the year, is plenty.
- The **mother's maiden name**, which banks have long used as a security question.
- The **home address**, especially since everyone will be at the service at a published time.
- **Pet names, hometowns and schools** written in a way that answers common security questions word for word.

STAY SAFE

An empty house during the service

Because the time of a funeral is published, some families ask a neighbor or friend to stay at the house during the service. It's a small kindness that brings real peace of mind.

Online memorial pages

Funeral homes and memorial websites often host a page where friends can leave messages. These are lovely. Keep an eye on them for anything odd, such as links asking for donations to unfamiliar places, and tell the funeral home if you see something that doesn't look right.

WHAT THIS DOES FOR YOU

Honor and protection, together

You can tell the whole story of a life, the people, the work, the laughter, without the handful of details a thief needs. Nobody reading it will ever notice what's missing.

PART 8

When to Call Bill & Your Cheat-Sheet

An honest word about when a hand is worth it, and one page that sums up the whole guide.

CHAPTER 25

When to Call Bill

I've written this guide so you can do most of this yourself. But it's a lot, and sometimes it's simply easier, or kinder, to have someone patient do the technical part with you. Here's my honest advice.

Times it's well worth a call

- **Setting up your plan**: Legacy Contact, Google's Inactive Account Manager, password manager emergency access, and a tidy inventory. We can do it together in one sitting.
- **Making sure the photos are safe**: checking that backups are really working, and copying everything to a drive for the family.
- **After a loss**: going through a loved one's phone and computer carefully, saving the photos, finding the subscriptions, and requesting access from Apple or Google.
- **Erasing devices properly** before they're passed on or recycled.
- **Something feels off**: a call, letter or pop-up you're not sure about. Ask before you act.

What working with me is like

I work at your pace, in your home here in Portage County or over a remote session, and I explain what I'm doing in plain words. I've been doing this kind of work for more than 30 years. I'll never rush a grieving family, and I'll tell you honestly when something is better handled by your attorney, your bank or the company itself.

FROM BILL

How to reach me

Call **(330) 200-8042** or book a time at **billshometech.com/book**. My help is $49 remote · $99 in your home. This guide is yours to keep and share, and no question is too small.

GOOD TO KNOW

You may meet Sophie

When you call or visit billshometech.com, you may be greeted by **Sophie**, my AI receptionist. She can answer quick questions and help you book a time. The actual help always comes from me.

Thank you for taking the time to look after the people you love, and for being so careful with the memories of those you've lost. Go gently, and remember I'm only a phone call away.

— Bill

CHAPTER 26

Your Digital Legacy Cheat-Sheet

The whole guide on one page. Print it and keep it with your important papers.

Planning ahead: the essentials

Account	What to do
Apple (iPhone, iPad, Mac)	**Settings** > your name > **Sign-In & Security** > **Legacy Contact**. Save the access key.
Google (Gmail, Photos, Android)	**myaccount.google.com/inactive**. Up to 10 people, your choice of data.
Facebook	Settings > Accounts Center > Memorialization: legacy contact, or delete.
Bitwarden	Web app > **Settings** > **Emergency access** (paid plan).
1Password	1Password.com > your name > **Manage Account** > **Save Emergency Kit**. Print it.
Microsoft, Amazon & others	No planning tool. Put the sign-ins in your envelope or password manager.
Photos	Backup on; second copy on a drive or shared album; Google Takeout for a full copy.

Write it down once

Keep handy	
My phone passcode is kept	_____
My password manager / master password is kept	_____
My Apple Legacy Contacts	_____
My Google Inactive Account Manager contacts	_____
My Facebook wish (memorialize / delete)	_____
Person handling my digital accounts	_____
My estate attorney	_____

After a death, in order

1. Keep their phone charged and their phone line active. Don't reset anything.
2. Find their plan: inventory, envelope, access key, letter of wishes.
3. Get several certified copies of the death certificate.
4. Make sure Social Security knows (funeral homes usually report it): 1-800-772-1213.
5. Protect their identity with the three credit bureaus; report misuse at IdentityTheft.gov.
6. Save the photos in two places before closing or erasing anything.
7. Request access or closure from Apple, Google, Facebook and the rest.
8. Stop subscriptions; let the executor close the bank and card accounts.
9. Erase devices before passing them on. Then cancel the phone line.
10. Unsure about anything? Call Bill at (330) 200-8042.

SCAM ALERT

The golden rule

Nobody real asks for gift cards, wire transfers, or a code sent to a phone. When in doubt, hang up and call back on a number you looked up yourself.