



Finding the Passwords When There's No List

When there is no kit and no list — where the logins hide, and the patient, lawful way to reach the accounts

————— **An Extended Guide · No. 1810** —————

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit — billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

1. The Whole Plan on One Page	4
2. The Common Reality of No List	4
3. What You Are Really Looking For	5
4. Where to Look First: the Web Browser	5
5. Saved Passwords in Google Chrome	6
6. Saved Passwords on an Apple Computer	7
7. Saved Passwords in Edge and Firefox	7
8. A Password-Manager App	8
9. The Notebook, the Drawer, the Sticky Notes	8
10. The Phone as a Trove of Logins	9
11. The Email Is the Master Key	10
12. Using the Email to Reset Other Accounts	10
13. Make the List as You Go	11
14. When There Is No Password to Find	11
15. Apple's Digital Legacy Process	12
16. Google's Deceased-User Request	13
17. Microsoft's Harder Door	13
18. Yahoo and AOL Accounts	14
19. Facebook, Instagram, and Social Accounts	14
20. Banks and Financial Accounts	15
21. If They Used a Password Manager's Legacy Feature	16

22. Don't Guess Yourself Into a Lockout	16
23. Don't Move Money From Their Account	17
24. When a Court Order Is Needed	17
25. The Death Certificate and Proof	18
26. When an Account Asks for a Code	18
27. Staying Organized With a Simple Log	19
28. What to Reach First	20
29. Scams That Target the Grieving	20
30. Guarding Against Identity Theft	21
31. Finding the Way to the Photos	21
32. Common Worries, Answered	22
33. Make a List Now, So No One Has to Hunt	22
34. If You Are Settling the Estate	23
35. If You Only Do Three Things	24
36. Finish the Job Soon	24
Everyday Cheat Sheet	25
A Picture to Follow Along	26
A Second Look	27
A Note From Bill	27
Your Visit — and My Promise	28

THE 60-SECOND VERSION

1. The Whole Plan on One Page

If you read only one page, read this. Here is the whole idea as a short checklist.

Most families discover, after a loss, that there is no tidy list of passwords anywhere. That is normal, and it is not hopeless. The passwords your loved one used are almost always saved somewhere — in a web browser, in an app, in a notebook by the desk. And the email, once you reach it, can reset most of the rest. Take a breath. There is a patient way through this.

- 1 Look in the web browser on the home computer for saved passwords.
- 2 Check for a password-manager app on the computer or phone.
- 3 Search the desk, drawers, and wallet for a notebook or written notes.
- 4 Reach the email first — it is the master key that resets other accounts.
- 5 For accounts you cannot reach, use each company's deceased-user process.
- 6 Keep a simple written list as you go, and never guess so often you lock an account.

GOOD TO KNOW

You do not need to find every password. If you can reach the email, you can reset most of the others from there, one at a time. The email is the thread that unravels the rest.

The rest of this guide walks each hiding place and each official path slowly, one page at a time. Take it at your own pace. There is no wrong speed, and no shame in asking for a hand.

THE REALITY

2. The Common Reality of No List

If you are holding a stack of accounts and no passwords, you are in very good company. Experts urge everyone to leave a password kit or a written list, but the honest truth is that most people never get around to it. So most families start exactly where you are: knowing the accounts exist, but not how to get in.

This guide is written for that reality, not the tidy one. It assumes there is no kit, no master list, and no neat set of instructions. The good news is that people leave trails without meaning to. Browsers remember logins. Phones stay signed in. Notes get scribbled. A patient search almost always turns up more than you expect.

- Most people never leave a formal password list — you are not alone.

- Passwords are usually saved somewhere, even without a plan.
- The email is the single most valuable account to reach first.
- Patience and a simple method beat any clever shortcut.

GOOD TO KNOW

The lack of a list feels like a locked door, but it is more like a house with the keys left in various drawers. The job is to find them, and they are usually findable.

WHAT TO FIND

3. What You Are Really Looking For

Before you start searching, it helps to know what counts as a find. You are not only hunting for a written word spelled out as a password. You are hunting for any way into an account: a saved login a browser will fill in, a phone already signed in, a recovery email you control, or a note that jogs the whole thing loose.

- Saved logins in a browser or an app, which fill themselves in automatically.
 - Devices already signed in — a computer, a phone, a tablet.
 - Written passwords in a notebook, on a sticky note, or in a wallet.
 - A recovery email or phone you can reach, to reset a password without knowing it.
- Keep that wider definition in mind. Many families get in not by finding a password at all, but by finding a browser that remembers it, or a phone that is still logged in. Those count just as much, and they are often easier to find than a written word.

GOOD TO KNOW

Before anything else, check whether the home computer or phone is already signed in to the email. An open session is the easiest door of all, and it may spare you the whole search.

THE BROWSER

4. Where to Look First: the Web Browser

For most people, the single richest hiding place is the web browser on the home computer — the program they used to visit websites, such as Chrome, Safari, Edge, or Firefox. Browsers offer to remember passwords as you go, and most people say yes without thinking. Over years, that quietly builds a complete list of logins, sitting right there.

If the computer itself is unlocked, or you know its password, this is the first place to look. Every major browser has a saved-passwords page that lists the websites and the logins,

and can reveal each password when you ask. The next few pages show exactly where that page is in each browser.

GOOD TO KNOW

A browser's saved-passwords list is often the closest thing to the master list your loved one never wrote. It can hold dozens of logins in one place, already organized by website.

- Browsers routinely save logins as people sign in to websites.
- The saved list can reveal both the username and the password.
- You usually need the computer unlocked, or its sign-in password, to view them.
- This is the first and often the most rewarding place to search.

CHROME

5. Saved Passwords in Google Chrome

Chrome is the most widely used browser, marked by a round, four-color icon. It keeps saved passwords in a built-in password area, tied to the person's Google account. If the computer is unlocked, you can open that area and see every login Chrome remembered, and reveal each password one at a time.

- 1 Open Chrome on the home computer.
- 2 Click the three-dot menu in the top corner, then open Settings.
- 3 Look for the section named Autofill, then Passwords, or Google Password Manager.
- 4 You will see a list of websites with saved logins.
- 5 Click a website, then the eye icon, to reveal the password — it may ask for the computer's sign-in password first.

TIP

If Chrome asks for the computer's password before revealing a saved one, that is the Windows or Mac sign-in password. Having that opens the whole list, so it is worth tracking down.

Because Chrome's passwords tie to the Google account, they may also appear on any other device signed into that same account. If you reach the Google account later, you can see the same list from anywhere — one more reason the email account matters so much.

SAFARI

6. Saved Passwords on an Apple Computer

On an Apple computer — a Mac — the usual browser is Safari, with a blue compass icon, and its saved passwords live in the system's own Passwords area. Apple guards these carefully, so you will generally need the computer's own sign-in password, or the fingerprint or face of the owner, to see them. That guarding is good security, and an obstacle after a death.

- 1 On the Mac, open the Passwords app, or open System Settings and find Passwords.
- 2 Sign in with the computer's own password when asked.
- 3 Browse the list of websites and saved logins.
- 4 Select any entry to reveal its password.
- 5 Note what you need, carefully, as you go.

WATCH OUT

If the Mac is locked and you do not know its password, do not keep guessing — repeated wrong tries can lock it harder. The Apple account recovery path, covered later, is the safer route in that case.

These saved passwords are the same ones that sync through iCloud Keychain across the person's Apple devices. That also means Apple will not hand them over through its bereavement process — the Keychain stays sealed — so finding them on an unlocked Mac is especially valuable.

EDGE & FIREFOX

7. Saved Passwords in Edge and Firefox

Two other common browsers are Microsoft Edge, with a blue-green swirl icon, and Firefox, with an orange fox. Both save passwords much as Chrome does, and both keep a settings page where you can view them if the computer is open to you. The menus differ slightly but the idea is identical.

- In Edge: open the three-dot menu, then Settings, then Profiles, then Passwords.
- In Firefox: open the menu, then Passwords, or Settings then Privacy & Security.
- Both show a list of websites and let you reveal each saved password.
- Both may ask for the computer's sign-in password before revealing one.

If you are not sure which browser your loved one used, check all of them. People often use one browser for one purpose and another for something else, so a login missing from one

may well be saved in another. It costs only a few minutes to look in each.

TIP

Look for a browser icon pinned to the taskbar or dock, or check which one opens by default. That tells you where your loved one did most of their browsing, and where the richest list is likely to be.

MANAGER APP

8. A Password-Manager App

Some people go a step beyond the browser and use a dedicated password-manager app — a locked vault that holds every login behind one master password. Common names include Bitwarden, 1Password, Dashlane, NordPass, LastPass, and Proton Pass. If your loved one used one, it is both very good news and a particular puzzle.

Good news, because everything is in one organized place. A puzzle, because that one place is locked behind a single master password you must find. Look for the app's icon on the computer or phone, and search the papers for that one master password, which many people do write down even when they write nothing else.

- A password manager holds every login behind one master password.
- Look for its app icon on the computer, the phone, or the browser toolbar.
- Search the papers and notebooks for that one master password.
- If it is open or signed in on a device, treat that session gently and do not sign out.

GOOD TO KNOW

Some password managers offer an emergency-access or legacy feature your loved one may have set up, naming a trusted person. If you were named, the manager itself may let you in. It is worth checking.

THE NOTEBOOK

9. The Notebook, the Drawer, the Sticky Notes

For all the technology, a great many people keep their passwords the old-fashioned way: written by hand. A little notebook in a desk drawer, a card in a wallet, a sticky note on the monitor, a page tucked into the back of an address book. Do not overlook these. They are often the plainest and most complete record of all.

- 1 Search the desk and its drawers, especially anything near the computer.

- 2 Check the wallet, the purse, and any small cards kept there.
- 3 Look under the keyboard, on the monitor, and in nearby drawers for sticky notes.
- 4 Flip through address books, planners, and the backs of notebooks.
- 5 Check a bedside table, a kitchen drawer, or wherever bills were handled.

TIP

People often keep a single page or card with their most important logins. Finding that one page can answer half your questions at once, so search thoroughly before moving to the harder paths.

Handwriting can be hard to read, and codes may be shorthand only your loved one fully understood. Take your time, and do not be discouraged by a scribble. Even a partial note — the right email address, a hint of a password — can be the clue that opens a door.

THE PHONE

10. The Phone as a Trove of Logins

The phone is often where a person's whole digital life is most alive, and if you can get into it, it holds a wealth of logins. Apps stay signed in. The phone's own saved-passwords feature holds website logins. And the messages and email on it can help reset still more. The companion phone guide covers getting into the handset itself.

If you know the phone's passcode, you have a powerful key. On an iPhone, the saved passwords live in Settings under Passwords. On an Android, they live in the Google account's password manager, reachable from Settings. Both can reveal saved logins once the phone is open, much as a browser does on a computer.

WATCH OUT

Do not repeatedly guess the phone's passcode. Too many wrong tries can lock the phone for a long time, or on some phones even wipe it. If you do not know the code, use the account paths instead.

- Apps on the phone are often still signed in — treat them gently.
- On an iPhone, saved passwords are in Settings, under Passwords.
- On an Android, they are in the Google account's password manager.
- A known passcode makes the phone one of the richest sources of all.

EMAIL FIRST

11. The Email Is the Master Key

Among everything you might find, one account stands above the rest: the email. Email is the master key, because almost every other account resets its password by sending a link to the inbox. Reach the email, and you can reach most of the rest, even for accounts you never found a password for at all.

So as you search, give the email address first priority. If a browser or phone is signed into it, or you find its password written down, you hold the key to the whole house. If you cannot find it, there is a companion guide devoted entirely to getting into a late spouse's email through each provider's official process.

GOOD TO KNOW

You do not have to find a password for every account. If you can open the email, you can reset most of the others from there, one at a time. Start with the inbox.

- Most accounts reset their password through the email.
- A browser or phone signed into the email is the richest find of all.
- Make reaching the email your first goal as you search.
- A separate guide covers reaching the email through official channels.

RESET THE REST

12. Using the Email to Reset Other Accounts

Once you can reach the inbox, you hold the master key, and a patient method opens one account after another. The trick is the humble 'forgot password' link that nearly every website offers. It sends a reset link to the email you now control, and from there you set a new password you record safely.

- 1 List the accounts you need, in order of urgency — money and bills first.
- 2 On each account's sign-in page, choose 'forgot password.'
- 3 Let it send the reset link to the email you now control.
- 4 Open the link from the inbox and set a new password you write down.
- 5 Record each one in your simple log as you go.

WATCH OUT

Be gentle with money accounts. Do not move funds or transact — simply gather what the estate needs. Moving money from a deceased person's account can complicate the estate and raise hard questions.

You will not reach every account this way; some use a second security step beyond email. A companion guide covers two-factor codes after a death. But the email alone unlocks a surprising number, and it is the right place to begin resetting.

KEEP A LIST

13. Make the List as You Go

As you find and reset logins, do the one thing your loved one did not: write them down in an orderly way. The list you build becomes the master list that was missing, and it will serve every other part of settling the estate. A simple notebook or a single sheet is all you need.

- 1 Start a page with one line per account.
- 2 For each, write the website, the login email, and the password.
- 3 Note how you got in — found it, reset it, or a device already signed in.
- 4 Mark the accounts still unreached, so you know what remains.
- 5 Keep the list sealed with the death certificates and estate papers.

TIP

Keep this list on paper, in a safe place, not in an email or a note on a phone. A sealed sheet in a drawer is beyond the reach of any online thief.

This list turns a scattered hunt into an orderly record. It tells you what you have handled and what is left, it keeps anything from slipping through, and it is a gift to anyone who helps you or picks up the work later.

OFFICIAL PATHS

14. When There Is No Password to Find

Some accounts will resist every search. No saved login, no written note, no way to reset through an email you can reach. For these, the companies themselves offer official paths for a deceased person's account. They are slower and ask for paperwork, but they are real doors, and the next pages walk through the big ones.

These official processes do not usually hand over a password. More often they provide a download of the data, or help close the account, or memorialize a profile. That is often all a family truly needs. Knowing what each company will and will not do saves you from waiting on an answer that was never coming.

GOOD TO KNOW

Companies almost never give out passwords, even to a surviving spouse. What they offer instead — a data download, account closure, memorialization — is usually enough for what families actually need.

- Official processes exist for accounts you cannot otherwise reach.
- They provide data, closure, or memorialization — rarely a password.
- Each asks for a death certificate and proof of your authority.
- They are slower, so start them early and let them run.

APPLE

15. Apple's Digital Legacy Process

For an Apple Account, the official path is Apple's digital legacy process. If your loved one named a Legacy Contact in advance, that person uses an access key and a death certificate to reach the account's data — the smoothest route. If not, Apple Support can sometimes help a family member with a death certificate and proof of relationship, though it reviews carefully.

- Best path: a Legacy Contact named in advance, with the access key.
- Otherwise: Apple Support with a death certificate and proof of relationship.
- Apple reaches iCloud photos and backups, but not the saved Keychain passwords.
- Approved access lasts up to three years, then the data is deleted.

A point worth repeating: Apple will not release the saved Keychain passwords, even to a Legacy Contact. Those are the very logins you are hunting, which is why finding them on an unlocked device matters so much. The companion phone guide covers the Apple paths in full detail.

TIP

If you gain access through Apple, download the photos and important data soon, because the access window closes after a few years. Save the irreplaceable things first.

GOOGLE

16. Google's Deceased-User Request

For a Google account — Gmail, Google Photos, and an Android phone's data — the official path is Google's request process for a deceased user. If your loved one set up Google's Inactive Account Manager in advance, naming you, you simply receive a download of the data they chose. If not, you use Google's request form.

- 1 Go to Google's help page titled 'Submit a request regarding a deceased user's account.'
- 2 Choose whether to close the account or to obtain data from it.
- 3 Enter the person's Google email and your own contact details.
- 4 Upload a death certificate and proof of your relationship or authority.
- 5 Submit and keep the confirmation; Google reviews each case carefully.

WATCH OUT

If you ask Google only to close the account, you may lose the chance to get the contents later. If you want the data, make the contents request first, before any closure.

Google will never give out the password. It may provide a data download or help close the account, after careful review. Complete paperwork and patience give you the best chance, and the download often holds exactly the photos and mail a family wants.

MICROSOFT

17. Microsoft's Harder Door

If your loved one used a Microsoft account — for Outlook.com mail or OneDrive files — the news is harder. Microsoft is generally unable to give account information to anyone but the account holder, and it has no next-of-kin form or legacy contact. If you find the password, you can sign in and even close the account. If not, the door is nearly shut.

Reaching the contents without the password generally requires a court order, and even that is not guaranteed. On the gentler side, a Microsoft account closes on its own after about two years of no sign-in, so if the contents are not essential, you can simply let it lapse rather than fight for it.

GOOD TO KNOW

If you cannot get into a Microsoft account and it holds nothing essential, letting it close on its own after about two years is a valid and restful choice.

- Microsoft has no next-of-kin form or legacy contact.

- With the password, you can sign in and close the account.
- Without it, contents generally need a court order.
- An untouched account closes by itself after about two years.

YAHOO & AOL

18. Yahoo and AOL Accounts

Older email addresses ending in yahoo.com or aol.com belong to accounts that lean heavily toward closure rather than release. Both companies will close a deceased person's account with a death certificate, and both only sometimes release the contents. An old, untouched account may also have been deactivated for long disuse, which clears the stored mail.

- Both close a deceased person's account on request, with a death certificate.
- Both emphasize closure over releasing the contents.
- A United States death certificate is generally required.
- Long-unused accounts may already have been deactivated and cleared.

If a Yahoo or AOL address is still the login for a bank or a bill, chase that connection even if the inbox itself holds little. The address can be more valuable as a recovery contact than for any old mail inside it. The companion email guide covers both services in full.

TIP

Before closing an old Yahoo or AOL account, redirect any bills or logins that still use it to an address you control. The address matters more than the dusty mail inside.

SOCIAL

19. Facebook, Instagram, and Social Accounts

Social accounts are a special case, because the goal is usually not to log in but to memorialize or close the profile. Facebook and Instagram both let a family member request that a profile be memorialized, which freezes it as a place to remember the person, or removed entirely. Neither will ever give out the login.

- Facebook can memorialize a profile with proof of death, such as an obituary link.
- A memorialized profile shows 'Remembering' and stops appearing in reminders.
- Removal requires closer family proof, such as a birth or death certificate.
- Instagram works much the same way, and also never gives out the login.

If your loved one set a legacy contact on Facebook in advance, that person can manage the memorialized profile, though even they cannot read private messages or log in. For most families, memorialization is the gentle and fitting choice, and it needs no password at all.

GOOD TO KNOW

Because social accounts are handled by memorialization or removal rather than login, you rarely need to hunt for their passwords at all. A separate guide covers Facebook and Instagram in depth.

BANKS

20. Banks and Financial Accounts

Bank and investment accounts are the ones where you should least want to find a password and log in. The proper path is not the website at all — it is the bank's own estate or bereavement process. With a death certificate and proof you are the executor or next of kin, the bank opens the account to you properly, which protects the estate far better than any login.

WATCH OUT

Do not log in and move money from a deceased person's bank account, even if you find the password. It can look as though the person acted after death and can seriously complicate the estate.

- Call the bank, report the death, and ask for its estate department.
- Provide a death certificate and proof you are the executor or next of kin.
- Let the bank open the account through its own process.
- Gather and account for the money; do not transact or transfer it.

So if you find a bank login in your search, note it in your list but do not act on it. The logins that matter most for the bank are not the website password but the papers that prove your authority. Those are the keys the bank actually wants to see.

EMERGENCY ACCESS

21. If They Used a Password Manager's Legacy Feature

It is worth a closer look at password managers, because several offer a built-in way to pass the vault to a trusted person. If your loved one used one and set this up, you may have a smooth and complete path to every login at once — the opposite of a scattered hunt.

- Bitwarden offers Emergency Access, where a named contact can request the vault after a waiting period.
- 1Password uses a printed Emergency Kit stored with the owner's papers.
- Several others, such as Dashlane and LastPass, offer emergency-access style features.
- If you were named, or find the Emergency Kit, you may reach the whole vault.

So before you resign yourself to a long hunt, check whether a manager was in use and whether you were set up as an emergency or legacy contact. Look too for a printed Emergency Kit among the important papers. Either one can hand you the whole set of logins in a single step.

GOOD TO KNOW

A companion guide covers setting up these emergency features in advance. If you are reading this for your own planning, that is the kindest list you can leave your family.

WHAT NOT TO DO

22. Don't Guess Yourself Into a Lockout

In the frustration of searching, it is tempting to try password after password, hoping to stumble on the right one. Please resist. Most accounts lock themselves after a handful of wrong tries, and some lock for a long time or demand extra verification you cannot provide. Guessing can turn a reachable account into a locked one.

- Repeated wrong passwords can lock an account, sometimes for a long stretch.
- A locked account is harder to recover than one you simply have not tried.
- Wrong guesses can also trigger security alerts that slow official recovery.
- If you do not have a login, use the reset or deceased-user path instead of guessing.

WATCH OUT

Never guess a phone passcode or an account password many times over. It is one of the few mistakes that can truly close a door for good. When you do not know it, stop and use the official route.

The patient path — find the saved login, or reset through the email, or use the official process — gets more people in than any lucky guess ever will. If you are tempted to keep trying, that is the moment to set it down and take a different door.

WHAT NOT TO DO

23. Don't Move Money From Their Account

This bears its own page, because it is the single most important rule when you do get into a financial account. However tempting or practical it seems, do not move money out of a deceased person's account, and do not keep using their cards. The estate must account for everything, and moving money yourself can create serious legal trouble.

The reason is simple. Once a person has passed, their accounts belong to the estate, to be settled in an orderly, documented way. Money moved after death can look as though the person acted when they could not, and it can complicate or even invalidate parts of the estate. Gather and record, but do not transact.

WATCH OUT

Do not pay bills, move funds, or make purchases from a deceased person's accounts, even to be helpful. Let the estate process handle the money. When in doubt, ask the attorney before you act.

If bills are coming due, speak with the estate's attorney or the bank about the proper way to handle them. There is almost always a correct channel, and using it protects you as much as it protects the estate.

COURT ORDER

24. When a Court Order Is Needed

For a few stubborn accounts — a Microsoft inbox most of all — no search and no polite request will open the contents. The provider requires a court order. This sounds daunting, but it is a known legal step, and you do not do it yourself. The estate's attorney petitions the probate court, which, if it agrees, issues an order the provider will honor.

A court order is not always worth the cost and effort, so weigh what is actually inside against the time and expense. Often the important things live somewhere reachable without one. Save the court-order route for the cases where the contents truly cannot be obtained any other way, and ask the attorney plainly whether it is likely to succeed.

TIP

Before pursuing a court order, ask the estate's attorney two questions: is it likely to work here, and is what is inside worth it? A short consult can save a long and costly detour.

- Some providers release contents only with a valid court order.
- The estate's attorney files it with the probate court; you do not do it alone.
- Even a valid order is not an absolute guarantee.
- Weigh the contents against the cost before pursuing one.

DOCUMENTS

25. The Death Certificate and Proof

Every official path asks for the same small stack of documents, so gather it once, early, and you are ready for each company instead of scrambling each time. A funeral home can usually help you order the certified copies you will need.

- A certified death certificate — the official state copy, not a home printout.
- Proof you are the surviving spouse, such as a marriage certificate.
- Court papers naming you as executor, or the will if it names you.
- Your own photo identification.

Order several certified death certificates at once, since each company may want its own copy, and the same stack serves the bank, the pension, and the insurance too. For online forms, a clear scan or photo of each document is usually enough; keep the paper originals for offices that insist on seeing them.

TIP

If you were named executor, say so plainly in every request. It is the word that most often moves a cautious company from a polite refusal to a path forward.

TWO-FACTOR

26. When an Account Asks for a Code

As you reset accounts through the email, you may hit a wall: after the password, the account wants a code sent to your loved one's phone. This is two-factor security, and it can stop even a rightful family member, because the code goes to a phone that may be locked. It is a common snag with known answers.

If you can keep the phone powered on and the line active, the code may appear on the lock screen where you can read it. If it comes from an authenticator app instead, it is harder. A companion guide covers two-factor codes after a death in full, including backup codes and the official recovery paths.

GOOD TO KNOW

Many phones show a text-message code right on the lock screen without unlocking. That small detail is often all that stands between you and finishing a reset.

Do not let a code wall convince you an account is lost. It is one more door with a known key. Keep the phone alive, look for printed backup codes, and lean on the two-factor guide when the codes get tangled.

ORGANIZED

27. Staying Organized With a Simple Log

Searching for passwords and resetting accounts is many small steps across many weeks. Without a record, it blurs together, and you lose track of what you have handled. The log you started earlier is worth tending carefully, because it becomes the backbone of settling the whole estate, not just the passwords.

- 1 Keep one line per account: the website, the login email, and the status.
- 2 Mark each as found, reset, closed, or still unreached.
- 3 Note any request you filed with a company and its reference number.
- 4 Record which accounts still charge a card, so they can be stopped.
- 5 Keep the log sealed with the death certificates and estate papers.

TIP

Review the log whenever you sit down to this work. It tells you at a glance what is done and what remains, so no account slips quietly through unnoticed.

A clear log pays off most on the day you must explain where things stand — to an attorney, a family member, or a helper. It turns a swirl of logins and requests into an orderly record anyone can follow and continue.

PRIORITIES

28. What to Reach First

Not every account needs urgent attention, and you do not have the energy to chase them all at once. It helps to work in order of what matters most, so the first days go to what counts and the rest can wait without worry.

- First: the email, because it unlocks resetting most other accounts.
- Next: banking, bills, and anything with automatic payments going out.
- Then: photos and memories, which are irreplaceable but not time-sensitive.
- Later: shopping, streaming, and social accounts, which can wait.

The accounts that quietly keep charging a card deserve early attention, because they do not stop on their own. The memories, precious as they are, are not going anywhere in the next few days, so there is no need to rush them. Let urgency, not sentiment, set the order of the work.

GOOD TO KNOW

Automatic payments are the ones that cause trouble if ignored, because they keep charging. Finding and stopping them early spares the estate from chasing refunds later.

STAY SAFE

29. Scams That Target the Grieving

It is a sad fact that criminals read obituaries and prey on the newly bereaved. In the weeks after a loss, you may get calls and messages designed to rush you into paying or handing over information. Knowing the common tricks ahead of time takes away their power, and none of them are your fault.

- A caller claims the deceased owed a debt and demands quick payment.
- Someone arrives with a 'package the deceased ordered' and asks for money.
- A caller posing as the funeral home demands a fee or the service will be delayed.
- A stranger befriends you online, often claiming their own recent loss, to win trust.

WATCH OUT

No legitimate company ever demands payment by gift card, wire, or a money app on an unsolicited call. That demand, by itself, is the proof that it is a scam. Hang up.

When something feels urgent and frightening, that is the scammer's whole game. Slow down. Hang up. Call the company back on a number you look up yourself. Taking your

time is a form of protection, especially while you are searching through sensitive accounts.

PROTECT IDENTITY

30. Guarding Against Identity Theft

A death, left unguarded, can open the door to identity theft, as thieves try to open credit or claim benefits in your loved one's name. The very accounts and documents you are gathering hold the details they want, so a few protective steps are worth doing alongside the search.

- 1 Notify the three credit bureaus and ask for a deceased flag on the file.
- 2 Keep obituaries short — leave out the full birth date, mother's maiden name, and home address.
- 3 Watch the mail and the inbox for new accounts that should not exist.
- 4 Opt out of data-broker listings where you can.

GOOD TO KNOW

The details thieves prize most — a birth date, a mother's maiden name, a home address — are exactly what some obituaries list. Keeping those private is a quiet, powerful protection.

It is one more task on a heavy list, but a small and finite one. Done once, it spares you a far larger headache later, and it protects the memory and good name of the person you lost.

THE PHOTOS

31. Finding the Way to the Photos

For many families, the photos are the whole reason for the search. They may be scattered — some on the phone, some in an email account's cloud, some on the computer itself. As you hunt for passwords, keep a special eye out for the way into the pictures, because they are the most irreplaceable thing of all.

- On an iPhone or Mac, photos may live in iCloud, reachable once you have the Apple account.
- On an Android, photos usually live in Google Photos, reachable through the Google account.
- On the computer itself, look in the Pictures folder and any backup drives.
- Once you reach them, copy them to a drive you can hold, and keep a second copy.

The old rule for precious files is three copies, on two kinds of storage, with one kept somewhere else. A lifetime of photos is exactly the thing worth that small extra effort. Once they are safely copied, you can breathe easier about the rest of the search.

GOOD TO KNOW

A companion guide covers reaching cloud photos in full. If the pictures are what matter most to you, it is worth starting there, even before the other accounts.

COMMON WORRIES

32. Common Worries, Answered

The same few questions come up for almost everyone searching for passwords that were never written down. Here are plain answers to the ones asked most.

- What if I never find the passwords? Reach the email and you can reset most accounts without them.
- Can I just guess? Please do not — repeated wrong tries can lock accounts and make recovery harder.
- Will companies give me the password if I prove I am the spouse? Almost never. They offer data, closure, or memorialization instead.
- Do I need a lawyer? Only for a stubborn account needing a court order, or a large estate. Most of this does not.

GOOD TO KNOW

The biggest mistakes are rushing and guessing. Patience, a careful search, and the official doors get more people in than any clever trick ever will.

If your worry is not here, it is almost certainly one a helper has met before. You are not the first to face a stack of accounts and no list, and you need not face it alone.

FOR COUPLES

33. Make a List Now, So No One Has to Hunt

If both partners are still here, the single kindest thing you can do is spare each other this search entirely. It takes one quiet afternoon to leave a simple list or set up a password manager, and it removes the hardest, most frustrating task a surviving spouse usually faces.

- Write down the main email and its password, and where it is kept.

- List the accounts that matter most, with their logins, on one sealed sheet.
- Consider a password manager with an emergency feature naming each other.
- Tell each other where the sealed list lives.

GOOD TO KNOW

Doing this together often surfaces small surprises — an account one of you forgot, a login neither remembers. An afternoon of it quietly simplifies your shared life too.

Planning for a day you hope is far off can feel tender. But couples who do it almost always feel relief rather than sadness — the quiet comfort of knowing the other will not spend grieving weeks hunting through drawers for a password.

FOR THE EXECUTOR

34. If You Are Settling the Estate

If you are the executor rather than the spouse, the search is the same, but your authority rests on the court papers naming you. Lead with those in every official request. Companies and banks respond far better to a clearly named executor than to a well-meaning relative without legal standing.

- 1 Keep the letters of administration or the will naming you close at hand.
- 2 Search the home thoroughly first — browsers, devices, notebooks, drawers.
- 3 Reach the email early, because it unlocks resetting many other accounts.
- 4 Keep a written log of every account, login, request, and conversation, with dates.

WATCH OUT

Work in order of urgency: money and anything still charging a card first, memories next, the rest after. You do not have to reach everything at once.

Be gentle with yourself. This is heavy work at a hard time, often for a grieving family counting on you. You do not have to be an expert — only patient, and willing to take it one careful step at a time.

A SIMPLE START

35. If You Only Do Three Things

Perhaps this all feels like a great deal. That is understandable, and you do not have to do it all at once. If you do only three things, do these, and you will have covered the ground that matters most.

- 1 Check the home computer's browser and any phone for saved logins and open sessions.
- 2 Reach the email first, because it is the master key that resets the rest.
- 3 Start a simple written list of every login you find, kept with the estate papers.

Those three steps either get you straight into most accounts or set the resets in motion, and they leave you with the orderly list your loved one never made. Everything else in this guide follows naturally once the email is in hand and the list is growing.

TIP

Done is better than perfect. Even checking the browser and reaching the email today puts you well ahead, and you can tackle the stubborn accounts at your own pace.

FINISH THE JOB

36. Finish the Job Soon

You now know the shape of the whole task. There may be no list, but the passwords are almost always somewhere — in a browser, an app, a notebook, or a phone. The email is the master key that resets the rest. And for the accounts that resist, the official deceased-user processes are real, if patient, doors. It is a lot to hold at a hard time, and you do not have to hold it alone.

If any step gives you pause — a browser you cannot open, an account that will not budge, a code you cannot get past, or simply the weight of facing it by yourself — that is exactly the kind of thing I help neighbors with. There is no question too small, and no grief I have not sat beside before.

GOOD TO KNOW

You do not have to remember all of it. You just have to remember you can call. Friendly, in-home help, and I come to you — (330) 200-8042.

Finding the passwords when there is no list is slow, patient work, but it is rarely hopeless. Search thoroughly, reach the email, keep a simple list, and lean on help where you need it.

The memories and the records are worth the patience. Take the time. Finish the job.

CHEAT SHEET

Everyday Cheat Sheet

Keep this page handy. It points you straight to what to do for each task. I want to... Do this
Check the browser Chrome, Safari, Edge, Firefox all keep a saved-passwords page Look
for a manager app A locked vault behind one master password — find that one password
Search the desk Notebooks, wallet cards, and sticky notes hold many written logins Reach
the email first It is the master key — resetting most other accounts runs through it Reset
with the email Use each account's forgot-password link to the inbox you control Use official
paths Apple, Google, Microsoft, Yahoo, AOL each have a deceased-user process Keep a
simple list One line per account, sealed with the estate papers Avoid the big mistakes Do
not guess into a lockout, and do not move money from their account Get help Call Bill:
(330) 200-8042

AT A GLANCE

A Picture to Follow Along

Where Passwords Hide

When there is no neat list, the passwords are almost always somewhere — you just have to look.

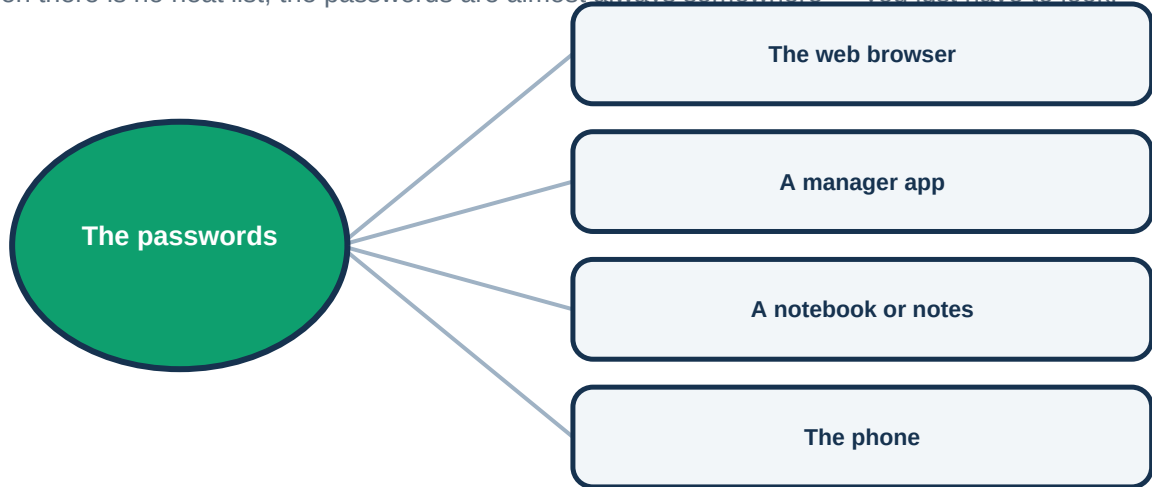


Illustration — a schematic. Set-up screens differ; each takes only a few minutes.

AT A GLANCE

A Second Look

From One Door to All

Do one box at a time — there is no rush, and no wrong pace.

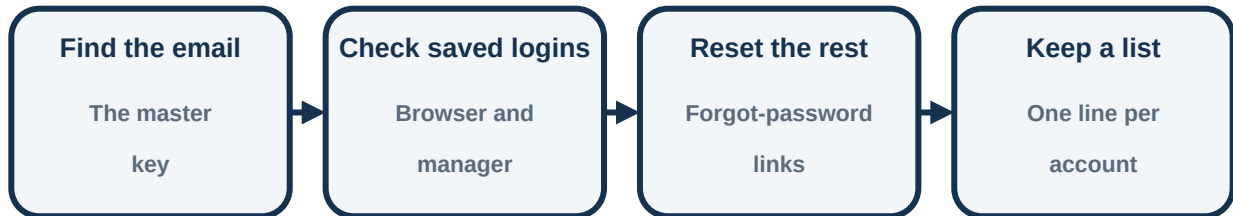


Illustration — a schematic. The order is a suggestion; do one box at a time.

A schematic of the plan — company steps vary; the order does not have to.

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.



HOW I CAN HELP

Your Visit — and My Promise

In-home visit — \$99 flat for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

Remote Support — \$49 for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full \$99. No questions, no awkwardness. That's how I'd want to be treated.

Call or text **(330) 200-8042** · Book a visit: billshometech.com/book · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.