



Locking Down Your Amazon Account

A calm, step-by-step security checkup

————— An Extended Guide · No. 1662 · PASSWORDS & SECURITY —————

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. Why your Amazon account is worth locking down	4
2. The checkup at a glance	4
3. Step one: a strong, unique password	5
4. Step two: turn on two-step verification	6
5. Choosing your second step: app or text	6
6. Step three: add a passkey	7
7. Reviewing your saved payment methods	7
8. Reviewing your saved addresses	8
9. Skimming your recent orders	9
10. Checking your signed-in devices	9
11. Reviewing recent login activity	10
12. What Amazon Household is	10
13. Setting up Household safely	11
14. Voice purchasing and smart speakers	12
15. Why scammers love to impersonate Amazon	12
16. The gift-card tell	13
17. The remote-access tell	13
18. Fake Amazon emails	14
19. Fake Amazon calls and texts	15
20. What a real Amazon message looks like	15
21. If you think your account was hit	16

22. Helping a spouse or parent lock down their account	17
23. Linked accounts and subscriptions	17
24. Keeping your email locked down too	18
25. A once-a-year checkup	18
26. Putting it all together	19
27. Frequently asked questions	19
Your Amazon Security Cheat Sheet	20
Plain-English Word List	21
A Picture to Follow Along	23
A Second Look	24
A Note From Bill	24
Your Visit — and My Promise	25

1. Why your Amazon account is worth locking down

It holds more of your life than you might think.

It's easy to think of Amazon as just a place to buy things, but your account quietly holds a surprising amount: the cards you pay with, every address you've ever shipped to, your phone number, your order history, and often a library of books, movies, and music. For many households it's also tied to the voice speakers and streaming devices around the home. All of that sits behind a single login.

That concentration is exactly why a thief would want in, and exactly why a few minutes spent locking it down pays off. Someone who gets into your Amazon account could order to a new address, drain a gift-card balance, read your personal details, or use the saved cards. The good news is that Amazon gives you solid tools to shut all of that down, and setting them up is more approachable than you'd expect.

GOOD TO KNOW

You don't have to do everything in this guide at once. Even just the first two steps — a strong password and two-step verification — put you ahead of the great majority of accounts a thief might try.

We'll go in a sensible order, from the most important protections to the finishing touches. Take it at your own pace, and lean on the cheat sheet at the front whenever you want the short version.

2. The checklist at a glance

What we'll do, so the whole thing feels manageable.

Before we dive in, here's the shape of the whole checklist, so none of it feels like a surprise. Think of it as five unhurried steps, each one making your account a little harder to break into. You can do them in one sitting or spread them over a few visits to the computer.

- 1 Give the account a strong, unique password.
- 2 Turn on two-step verification.
- 3 Add a passkey for easy, password-free sign-in.
- 4 Review what's saved — your cards and your addresses.
- 5 Look over your orders, devices, and recent sign-ins.

After those five, we'll cover sharing safely with family through Amazon Household, and then spend real time on spotting the fake 'Amazon' scams, because those are what actually catch most people. By the end you'll have both a locked-down account and a clear eye for the tricks aimed at it.

TIP

Nearly everything here lives in one place on Amazon: 'Account & Lists,' then a section called 'Login & security.' If you can find that page, you can do most of this checkup.

3. Step one: a strong, unique password

The foundation everything else rests on.

The first and most important step is a strong password that you use only for Amazon. The danger isn't that someone guesses your password out of thin air — it's that you've used the same one somewhere else that got breached, and thieves try that leaked password on Amazon. A password used only here can't be stolen from anywhere else.

To change it, go to 'Account & Lists,' open 'Login & security,' and choose Edit next to Password. Make the new one long — a passphrase of a few unrelated words is both strong and easy to type. Then store it in your password manager, or write it in your notebook, so you never have to hold it in your head.

- 1 Open Account & Lists, then 'Login & security.'
- 2 Choose Edit next to Password.
- 3 Set a long passphrase used nowhere else.
- 4 Save it in your password manager or notebook.

WATCH OUT

If you've ever used your Amazon password on another site, treat it as compromised and change it here. Reused passwords are the single most common way accounts get taken over.

4. Step two: turn on two-step verification

The protection that stops a stolen password cold.

If you do only one thing from this guide, make it this. Two-step verification — Amazon's name for two-factor — adds a second check when you sign in, so that even if a thief has your password, they still can't get in without the second step, which lives on your phone. It is the single biggest upgrade to your account's safety.

You'll find it in the same 'Login & security' page, usually labeled 'Two-Step Verification' with a Turn On or Edit button. Amazon will walk you through linking it to your phone. From then on, signing in on a new device asks for both your password and a short code, which only you can get.

- 1 Open 'Login & security' and find Two-Step Verification.
- 2 Choose Turn On or Edit.
- 3 Follow the prompts to link it to your phone.
- 4 Save any backup method it offers.

GOOD TO KNOW

Turning this on doesn't mean entering a code every single time. Amazon lets you trust your own devices, so you'll mostly be asked only when signing in somewhere new — which is exactly when you'd want the extra check.

5. Choosing your second step: app or text

Both work; one is a little sturdier.

When you set up two-step verification, Amazon offers a choice for how you get the code. The two common options are a text message to your phone, or a small 'authenticator' app that shows a fresh code every little while. Both are far better than no second step at all, so don't let the choice stall you.

If you want the simplest thing, a texted code is perfectly fine and familiar. If you want a touch more protection, an authenticator app is sturdier, because codes sent by text can — in rare, targeted cases — be intercepted by a determined crook. Many people start with text and move to an app once they're comfortable.

- Text message — simplest and familiar; a big step up from nothing.
- Authenticator app — sturdier, since the code lives only on your phone.

- You can set up both, so one is a backup for the other.

TIP

My guide comparing two-factor by app, text, and email goes deeper on this choice. For Amazon, the honest answer is: pick whichever you'll actually turn on, because any second step beats none.

6. Step three: add a passkey

Password-free sign-in that's very hard to steal.

A passkey is the newest and, in some ways, the easiest way to sign in. Instead of typing a password, you confirm with your face, your fingerprint, or your device's PIN — the same gentle unlock you already use for your phone. The passkey itself never leaves your device, which is what makes it so hard for a scammer to steal: there's no password to phish out of you.

Amazon lets you add a passkey from the same 'Login & security' page. Adding one doesn't remove your password; it simply gives you a quicker, safer way to get in. For many folks, a passkey turns signing into Amazon into a one-touch affair while quietly raising their security at the same time.

- 1 Open 'Login & security' and look for Passkey.
- 2 Choose to add one and follow the prompts.
- 3 Confirm with your face, fingerprint, or device PIN.
- 4 Keep your password as a backup way in.

GOOD TO KNOW

My guide on setting up passkeys across Google, Apple, Microsoft, and Amazon walks through this in detail. A passkey is one of the strongest protections there is, and it's genuinely simple to use once it's on.

7. Reviewing your saved payment methods

Make sure only your own cards are on file.

With your sign-in locked down, turn to what's saved inside the account, starting with your payment methods. Amazon keeps your cards on file so checkout is quick, which is convenient — but it also means you'll want to glance over that list now and then to be sure nothing unfamiliar has crept in and nothing expired is cluttering it up.

- 1 Open 'Account & Lists,' then 'Payment options.'
- 2 Look over every card and payment method listed.
- 3 Remove any card you don't recognize or no longer use.
- 4 Update expired cards so legitimate orders don't fail.

A card you don't recognize is a red flag worth taking seriously — remove it and change your password. More often, though, you'll simply find an old expired card or two worth tidying away. Either way, a quick look keeps the list clean and gives you peace of mind about what's on file.

WATCH OUT

If you spot a payment method you never added, treat the account as compromised: change your password, turn on two-step if it isn't already, and check your recent orders carefully.

8. Reviewing your saved addresses

A sneaky place thieves try to hide.

Saved addresses are worth a careful look because they're where a clever thief does their damage quietly. Someone who gets into your account might add their own address and ship your orders there, hoping you won't notice an extra entry in a list you rarely check. Giving the address list a glance closes that door.

- 1 Open 'Account & Lists,' then 'Your Addresses.'
- 2 Read through every address saved there.
- 3 Delete any address that isn't yours or a known recipient.
- 4 Confirm your default shipping address is the right one.

Everything should be an address you recognize — your home, a relative, a workplace. An unfamiliar address, especially set as the default, is a strong sign someone's been in the account, and it calls for a password change and a look at recent orders.

GOOD TO KNOW

Thieves favor the address trick because it's easy to overlook. You buy things all the time, so an order slipping out to a strange address can hide in plain sight. A yearly glance at this list is a simple safeguard.

9. Skimming your recent orders

The quickest way to spot trouble early.

Your order history is a plain, honest record of what's actually happening in the account, which makes it one of the best places to catch trouble. A quick skim down your orders will show you at a glance whether everything there is something you or your household actually bought.

- Open 'Returns & Orders' from the top of the page.
- Scan for anything you don't recognize buying.
- Check where recent orders were shipped.
- Watch for digital items — gift cards, app purchases — you didn't make.

If every order is yours, wonderful — close the page reassured. If something's off, don't panic: note what it is, change your password, and we'll walk through the recovery steps later in this guide. Catching a stray order early is often the first sign of a problem, and acting on it quickly keeps the damage small.

TIP

Digital purchases are the easiest for a thief to cash in quickly, since there's nothing to ship. Give any unexpected gift-card or app purchases an extra-careful look.

10. Checking your signed-in devices

See every phone, tablet, and TV that's logged in.

Over the years your Amazon account gets signed into a lot of places — phones, tablets, computers, smart TVs, streaming sticks, and voice speakers. Each of those is a door into your account, and old or unfamiliar ones are worth clearing out. Amazon keeps a list of the devices tied to your account that you can review.

You'll usually find this under a heading about your devices or your content and devices, reached from 'Account & Lists.' Look down the list for anything you don't recognize — an old phone you've replaced, a device in a place you've never been. Removing those is a tidy way to shrink the number of open doors.

- 1 From 'Account & Lists,' find the devices or content-and-devices area.
- 2 Read through the list of signed-in devices.
- 3 Remove old devices you no longer own.

4 Flag anything you don't recognize at all.

GOOD TO KNOW

It's normal for this list to be longer than you expect, full of gadgets you'd forgotten. That's not alarming by itself — the goal is just to remove the ones that are truly gone or unfamiliar.

11. Reviewing recent login activity

A look at where and when your account was used.

Beyond the device list, it's worth knowing that Amazon offers tools to review how your account has been accessed and to secure it if something seems wrong. If you ever have a nagging worry that someone's been in your account, these are the places to look for reassurance or for the first sign of a problem.

The surest, simplest response to any such worry is to sign out of all devices at once and then sign back in yourself. That single action boots out anyone who shouldn't be there, and because you've set up two-step verification, they can't follow you back in. It's a clean reset whenever you feel uneasy.

- Look for a 'secure your account' or sign-out-everywhere option in Login & security.
- Signing out of all devices ejects anyone else immediately.
- Sign back in yourself, protected by your password and second step.

TIP

'Sign out of all devices' is your emergency brake. Any time something feels off — a strange order, an odd email — pulling it costs you nothing but a few fresh sign-ins and instantly clears out an intruder.

12. What Amazon Household is

Sharing benefits between two adults in a home.

Amazon Household is a feature that lets two adults in the same home share certain benefits — things like Prime shipping and some digital content — without sharing a single login. It can be genuinely useful for spouses or a parent and an adult child under one roof. But it shares more than people expect, so it's worth understanding before you switch it on.

The catch that surprises folks is payment. When two adults are linked in a Household, each can typically use the other's saved payment methods to make purchases. That's fine

between people who fully trust each other and talk about spending, but it's not something to set up casually or with someone you're not completely comfortable sharing a wallet with.

WATCH OUT

Linking a Household means the other adult can buy things using your cards. Only set this up with someone you'd happily hand your wallet to — and make sure you both understand how the shared payment works.

If that sharing fits your situation, Household is a nice convenience. If it doesn't, you're under no obligation to use it, and keeping accounts separate is perfectly sensible.

13. Setting up Household safely

How to share the good parts without the risk.

If you do want to use Amazon Household, a little care makes it work smoothly. The key is to go in with eyes open about what's shared, to link only with someone you trust completely, and to keep an occasional eye on the shared account just as you would your own.

- Only link with a spouse or close family member you fully trust.
- Talk openly about how shared payment will be used.
- Each adult keeps their own login and their own strong password.
- Review orders now and then, since purchases can be made on shared cards.
- Know how to leave the Household if your situation changes.

Set up this way, Household gives a couple or a close family the shared Prime benefits and content they want, while each person keeps their own private account and sign-in. It's the sharing done thoughtfully, rather than by handing over a password.

GOOD TO KNOW

Sharing a Household is far safer than sharing one password and login. My guide on sharing passwords safely with a spouse or caregiver covers the broader principle, and it applies here too.

14. Voice purchasing and smart speakers

Closing an easy door you may not use.

If you have a voice speaker in the home, it's likely tied to your Amazon account and may be able to place orders by voice. That's handy for some and unwanted for others — and it's a door worth thinking about, since anyone who can speak to the device, including guests or grandchildren, could potentially order with it.

You can turn voice purchasing off entirely, or add a spoken code that must be given before an order goes through. Either option lives in the settings of the app that runs your speaker. If you never buy by voice, simply switching it off removes the possibility of an accidental or mischievous order.

- Turn voice purchasing off if you don't use it.
- Or set a voice code required before any order completes.
- These settings live in the app that controls your speaker.

TIP

If a grandchild has ever 'ordered' something by chatting with a speaker, this is the setting to fix. A quick change prevents the surprise parcel — and the hassle of sending it back.

15. Why scammers love to impersonate Amazon

The setup for the most important part of this guide.

Here's a truth worth sitting with: for most people, the real danger to their Amazon account isn't a hacker breaking in — it's a scammer talking them into opening the door themselves. Because nearly everyone has an Amazon account, pretending to be Amazon is one of the most common tricks going, and it fools sharp people every day.

The scam usually arrives as an email, a text, or a phone call claiming there's a problem: a 'suspicious order,' a 'locked account,' a 'refund waiting.' The aim is always the same — to rattle you into acting fast, so you hand over your password, your card, or control of your computer before you've had a moment to think. The next several pages are about seeing these for what they are.

GOOD TO KNOW

There's no shame in nearly falling for one of these — they're designed by professionals to be convincing. The protection isn't being clever; it's knowing the handful of tells, which never change.

Learn the tells once and they'll serve you for life, because scammers can change the wording but not the underlying trick. Let's go through them plainly.

16. The gift-card tell

The one rule that defeats most Amazon scams.

If you remember just one thing from this guide, let it be this: Amazon will never ask you to pay for anything, or to 'verify' or 'protect' your account, using gift cards. Not Amazon gift cards, not any other brand. A request to buy gift cards and read off the numbers is a scam one hundred times out of a hundred. There are no exceptions.

Scammers love gift cards because once you read them the numbers, the money is gone and can't be traced or reversed, the way a bank transfer sometimes can. So they invent urgent reasons you must pay this way: a bill, a fine, a fee to 'release' a refund. The moment gift cards enter the conversation, you can stop listening — you've caught a thief.

TIP

Anyone — on the phone, by email, or by text — who tells you to buy gift cards and share the numbers is a scammer, no matter how official they sound or how urgent they make it. Hang up or delete the message.

This single rule, held firmly, defeats a huge share of the frauds aimed at shoppers. It's simple, it never changes, and it's worth repeating to everyone you care about.

17. The remote-access tell

Never let a 'helper' into your computer.

The second rule is just as firm: a real Amazon representative will never ask to take remote control of your computer. Scammers, on the other hand, love this move. They'll claim they need to 'fix' a problem, 'process your refund,' or 'remove a virus,' and ask you to install a program or read them a code that hands them control of your screen.

Once they're in, they can watch you log into your bank, move money, plant real malicious software, or lock you out entirely. It is one of the most damaging traps there is, precisely because it feels like help in a stressful moment. Treat any request for remote access as the end of the conversation.

TIP

If someone claiming to be from Amazon asks to connect to your computer, or to install an app so they can 'help,' refuse and hang up. No legitimate Amazon support needs control of your machine.

If you're ever unsure whether a genuine support session is appropriate, stop and ask someone you trust, or call me first. It's always free to check before you let anyone in.

18. Fake Amazon emails

What to look for before you click anything.

Fake Amazon emails are everywhere, and many are convincing, complete with logos and tidy formatting. But they share tells that give them away once you know to look. The golden habit is never to act directly from the email — no clicking links, no calling the number it gives — but to go to Amazon yourself and check.

- A sense of urgency or threat — 'your account will be closed,' 'act now.'
- A link that, when you hover over it, doesn't go to amazon.com.
- Requests for your password, full card number, or Social Security number.
- Odd greetings, clumsy wording, or an address that isn't quite Amazon's.

The safe response is always the same: don't click. Open your browser or the Amazon app, sign in the way you normally do, and look for any real notice there. If there's a genuine problem, it will show up in your actual account. If there's nothing, the email was a fake you can delete.

WATCH OUT

A real order confirmation or shipping notice never needs your password. If an 'Amazon' email asks you to log in through its link to 'confirm' or 'verify,' that link is the trap. Go to Amazon yourself instead.

19. Fake Amazon calls and texts

The phone and your messages are favorite routes.

Scammers increasingly reach out by phone and text, because a live voice or a quick message feels more urgent and personal than an email. A common version is a recorded call or a text about a 'suspicious order' you didn't place, urging you to press a button or call a number 'to cancel it.' The order is imaginary; the goal is to get you on the line with a scammer.

- A call or text about an order or charge you don't recognize, urging quick action.
- A number to call that didn't come from Amazon's own app or website.
- Pressure to 'confirm' details, make a payment, or stay on the line.
- A text with a link to 'track,' 'cancel,' or 'verify' — don't tap it.

The response mirrors the email rule. Don't press the button, don't call the number they gave, don't tap the link. Hang up, and if you want to be sure, open the Amazon app yourself and check your orders. A real issue will be visible there; a fake one simply won't exist.

WATCH OUT

Amazon does not call people out of the blue demanding immediate action on a 'suspicious order.' A high-pressure call like that is the scam itself — hang up and check your account on your own.

20. What a real Amazon message looks like

So the genuine ones don't rattle you.

Knowing the fakes is half the battle; it also helps to know what the real thing looks like, so a genuine notice doesn't send you into a worry. Real Amazon messages tend to be calm and specific. They confirm an order you actually placed, tell you something has shipped, or note a delivery — and they never demand your password or threaten you.

- Real messages reference specific orders you recognize.
- They don't create panic or threaten to close your account in minutes.
- They never ask for your password, full card number, or gift cards.
- Anything truly important also appears inside your account when you log in yourself.

The surest test of all cuts through every doubt: whatever a message claims, close it and open Amazon yourself. Your real account is the single source of truth. If the notice is

genuine, you'll see it there; if it isn't, you've lost nothing by checking.

TIP

Amazon keeps a record of its real messages to you inside your account, often under a message center. Comparing a suspicious email against that record is a quick way to tell real from fake.

21. If you think your account was hit

A calm, clear order of operations.

If you ever believe someone has gotten into your Amazon account — an order you didn't place, a strange address, a payment method you don't recognize — don't panic. There's a clear sequence that shuts the intruder out and limits any harm, and you can work through it calmly.

- 1 Change your Amazon password straight away to something strong and new.
- 2 Turn on two-step verification if it isn't already on.
- 3 Use 'Sign out of all devices' to eject anyone else.
- 4 Review your orders, payment methods, and addresses, removing anything unfamiliar.
- 5 Contact Amazon through the Help section of its own site or app — not a number from a suspicious message.
- 6 If a card was used, call your bank or card company to watch or stop the charge.

Working through these in order closes the door, pushes the intruder out, and cleans up anything they touched. The two-step verification you set up earlier is what stops them from simply coming back once you've changed the password.

WATCH OUT

Reach Amazon's help only through the app or by typing their address yourself. Searching for an 'Amazon support number' online can turn up fake numbers that scammers have planted to catch worried people.

22. Helping a spouse or parent lock down their account

The same checkup, done together.

If you look after the online life of a spouse or an older parent, their Amazon account deserves the same checkup — and the scam awareness matters even more, since older shoppers are heavily targeted by the fake-Amazon calls and texts. The goal is an account that's locked down and a person who knows the handful of tells by heart.

- Walk through the five steps together: password, two-step, passkey, saved details, orders.
- Store their password in a shared family password manager so you can help if they're stuck.
- Drill the two unbreakable rules: no gift cards, no remote access, ever.
- Agree that when in doubt, they'll close the message and call you before acting.

That last agreement — 'call me before you act' — is worth more than any setting. Most scams rely on catching someone alone in an anxious moment. A standing habit of pausing to call a trusted person breaks the spell nearly every time.

TIP

My guides on family password managers and emergency access pair naturally with this, covering how to keep a loved one's logins reachable by the right people and no one else.

23. Linked accounts and subscriptions

The quiet charges and connections worth a look.

Beyond the obvious cards and addresses, an Amazon account gathers a few quieter connections over the years: subscriptions that renew on their own, 'Subscribe & Save' deliveries, and other services linked to your login. None of these is a danger in itself, but a periodic glance keeps you in command of what's running and what's being charged.

- Review your memberships and subscriptions for anything you've forgotten.
- Check 'Subscribe & Save' deliveries so nothing arrives unwanted.
- Look over any other services signed in with your Amazon account.
- Cancel what you no longer use, so there's less tied to the account.

A thief who got in briefly might also start a subscription to test the account, so an unfamiliar membership is worth the same caution as a strange order. More often you'll simply find something you meant to cancel long ago — a tidy win either way.

GOOD TO KNOW

Fewer loose connections means a simpler account to watch over. Trimming subscriptions you don't use is good for both your peace of mind and your wallet.

24. Keeping your email locked down too

The account behind the account.

Here's a connection that's easy to miss: your Amazon account is only as safe as the email address attached to it. That's because the 'forgot password' path sends a reset link to your email. Anyone who controls your inbox can reset your Amazon password and walk right in, no matter how strong that password is.

So locking down Amazon isn't quite finished until your email is locked down as well. The same principles apply there: a strong, unique password and two-step verification on the email account itself. Think of your email as the master key, and Amazon as one of the many doors it can open.

- Give your email account its own strong, unique password.
- Turn on two-step verification for your email.
- Treat any 'reset your Amazon password' email you didn't request as suspicious.

TIP

My guide 'Your Email Is the Master Key' is the natural companion to this one. Locking down your inbox protects not just Amazon but nearly every account you own.

25. A once-a-year checkup

Five minutes to keep it all buttoned up.

Your Amazon security doesn't need constant attention, but a short yearly look keeps it honest and catches anything odd early. Tie it to something you already do each year so it's easy to remember — tax season, a birthday, the turn of the year.

- 1 Confirm two-step verification and your passkey are still on.
- 2 Skim your saved cards and addresses for anything unfamiliar.
- 3 Glance down recent orders for purchases you don't recognize.
- 4 Clear out old signed-in devices you no longer own.
- 5 Refresh the scam rules in your mind — no gift cards, no remote access.

That's the whole routine. In a few minutes you've confirmed the account is still well protected and reminded yourself of the tricks aimed at it. Small, steady attention like this is what keeps a locked-down account locked down.

GOOD TO KNOW

If you share an Amazon Household, make this the moment to glance over the shared side too, so both accounts stay as tidy and safe as your own.

26. Putting it all together

The whole plan in one calm breath.

Let's bring it home. Locking down your Amazon account comes down to a short, doable list: give it a strong, unique password, turn on two-step verification, add a passkey, and glance over what's saved and what's been ordered. Share with family through Household thoughtfully if it suits you. And above all, hold the two unbreakable scam rules.

- 1 Strong, unique password — stored safely, not in your head.
- 2 Two-step verification on — the single biggest protection.
- 3 A passkey added for quick, hard-to-steal sign-in.
- 4 Saved cards, addresses, orders, and devices reviewed.
- 5 Household shared only with someone you fully trust.
- 6 No gift cards, no remote access — ever, no matter who asks.

Do those, and your account is well protected and you're ready for the tricks aimed at it. No gadget, no subscription — just a handful of settings and a clear eye for the scams.

GOOD TO KNOW

If any single step here feels like one too many, you don't have to do it alone. Walking through exactly this, at your kitchen table or over a screen-share, is one of the most common things I help folks with.

27. Frequently asked questions

Quick answers to the things people ask most.

Does Amazon ever ask for payment in gift cards? Never. Any such request, by phone, email, or text, is a scam with no exceptions.

Will a real Amazon agent ask to access my computer? No. A request for remote access to your computer is always a scam, however helpful it sounds.

Is two-step verification a nuisance to use? Not really. Amazon lets you trust your own devices, so you'll mostly be asked only when signing in somewhere new.

What's the difference between a passkey and a password? A passkey uses your face, fingerprint, or device PIN and never leaves your device, so there's nothing for a scammer to phish out of you.

Is Amazon Household safe? It's safe with someone you fully trust, but remember it lets the other adult buy using your saved cards, so set it up knowingly.

TIP

If any of this feels like one step too many, that's exactly the kind of thing I can sit down and sort out with you — in person or remotely — in under an hour.

CHEAT SHEET

Your Amazon Security Cheat Sheet

Keep this by the computer. It's the whole checkup on one page, plus the scam tells to remember.

The security checkup, in order

- 1 Set a strong, unique password used nowhere else.
- 2 Turn on two-step verification (Login & Security settings).
- 3 Add a passkey so your face or fingerprint can sign you in.
- 4 Review saved cards and addresses; remove any you don't recognize.
- 5 Skim recent orders and your signed-in devices.

Where to find the settings

- Account & Lists, then 'Login & security.'
- Payment options for saved cards.
- Your Addresses for saved addresses.
- Content library or device list for signed-in devices.

The scam tells — always true

- Amazon will NEVER ask you to pay with gift cards.
- Amazon will NEVER ask for remote access to your computer.

- Amazon won't call out of the blue about a 'suspicious order' and demand you act.
- When unsure, close the message and open the Amazon app yourself.

If something's wrong

- Change your password, then sign out of all devices.
- Check orders and payment methods for anything you didn't do.
- Call Bill's Home Tech at (330) 200-8042 if you'd like a hand.

WORDS TO KNOW

Plain-English Word List

Two-step verification — A second check at sign-in, on top of your password — usually a code or a tap on your phone — so a stolen password alone can't get in. Amazon's name for two-factor.

Passkey — A newer, password-free way to sign in using your face, fingerprint, or device PIN. Very hard for a scammer to steal because it never leaves your device.

Authenticator app — A small app on your phone that shows a fresh six-digit code every little while. A sturdier second step than a texted code.

Login & security — The Amazon settings page where you change your password, turn on two-step verification, and manage passkeys.

Amazon Household — An Amazon feature that lets two adults in a home share certain benefits. Convenient, but it shares more than people expect, so set it up with care.

Saved payment method — A card or bank detail Amazon keeps on file so checkout is quick. Worth reviewing so nothing unfamiliar lingers there.

Phishing — A fake message pretending to be Amazon, built to trick you into giving up your password or payment details. Often arrives by email or text.

Gift-card scam — A fraud where a fake 'Amazon' agent insists you pay or 'verify' with gift cards. Amazon never does this — it's always a scam.

Remote access — Letting someone control your computer from afar. A real Amazon agent will never ask for this; scammers do, to raid your accounts.

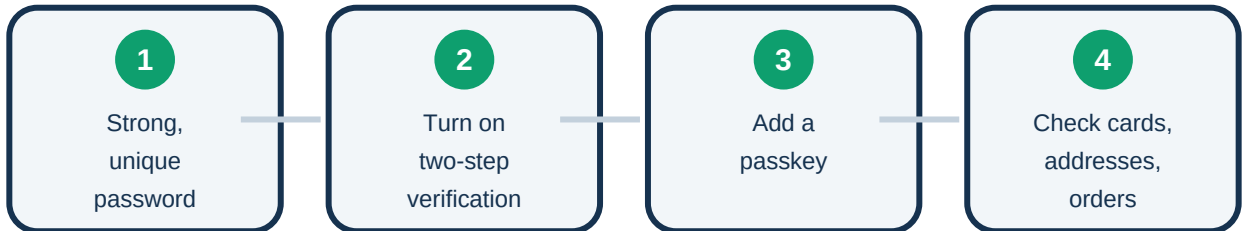
Sign out of all devices — An Amazon option that signs your account out everywhere at once — the fastest way to boot out anyone who shouldn't be there.

AT A GLANCE

A Picture to Follow Along

The Amazon Security Checkup

Four moves that lock down your account.



A strong password plus two-step is the heart of a safe Amazon account.

Illustration - do these in order and the account is well protected.

AT A GLANCE

A Second Look

Real Amazon vs. a Fake 'Amazon'

How to tell a genuine message from a scam.

Real Amazon	Fake 'Amazon'
- Never asks for gift cards - Never needs remote access - Changes made in the app - No pressure, no threats	- Demands gift cards - Wants to 'help' remotely - Urgent, scary wording - Links to odd websites

Amazon will never ask for gift cards or remote access - that's always a scam.

Illustration - when in doubt, close the message and open the app yourself.

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.