



A One-Page Scam Playbook for the Whole Family

One simple plan, shared by everyone — the whole family's defense on a single page.

————— An Extended Guide · No. 1641 · SAFETY —————

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.

The 60-Second Version	4
1. Why One Plan Beats a Hundred Scams	4
2. The Shape Every Scam Shares	5
3. Habit One — Verify First	6
4. Habit Two — Never Rushed, Never Secret	7
5. Habit Three — The Family Safe Word	7
6. Habit Four — Know the Payment Red Flags	8
7. Habit Five — The Open Door	9
8. The One-Page Playbook Itself	10
9. Setting It Up as a Family	11
10. The Playbook Against the Grandchild Scam	11
11. The Playbook Against Impersonation	12
12. The Playbook Against Online Scams	13
13. Teaching Every Generation	14
14. Keeping the Plan Alive	15
15. When a Scam Gets Through Anyway	15
16. The Devices Part of the Plan	16
17. A Note for Those Who Live Alone	17
18. Why This Protects Against Tomorrow	18
19. Questions People Ask Me	19
20. Your Playbook, in Five Minutes	19

21. Reporting It — and Why It Helps 20

22. When to Just Call Me 21

23. Contact Card & a Warm Close 21

The One-Page Playbook 22

A Picture to Follow Along 23

A Second Look 24

A Note From Bill 24

Your Visit — and My Promise 25

SUMMARY

The 60-Second Version

Your family does not need to track every scam. You need one shared plan built on a few sturdy habits: verify any urgent money request on a channel you already trust; never act while rushed or keep a money decision secret; set a family safe word for 'loved one in trouble' calls; never pay by gift card, wire, or crypto at a caller's direction; and keep an open, no-judgment door so anyone can check a worrying message with the family. Write it on one page, keep it by the phone, and the whole family is protected.

- 1 Verify first: confirm urgent requests on a number you already have.
- 2 Never rushed, never secret, about money.
- 3 Set a family safe word, private and never posted online.
- 4 Never pay by gift card, wire, or crypto for a caller or message.
- 5 Keep the door open: anyone can check a worrying message, no judgment.

GOOD TO KNOW

One shared plan beats a hundred memorized scams, because it responds to the shape of a scam — urgent, secret, odd payment — not its ever-changing disguise. It even protects against scams not yet invented.

1. Why One Plan Beats a Hundred Scams

The idea behind the playbook.

In more than thirty years of helping families across Portage County with their technology, I have learned that no one can keep up with every scam. New ones appear constantly, the old ones mutate, and the AI-powered fakes get better every year. Trying to protect your family by memorizing a growing list of individual scams is a losing game — there are too many, they change too fast, and in the frightening moment, no one remembers the right item from a long list anyway.

So this guide takes a different approach, and I think a better one: instead of a hundred scams, one plan. The great majority of scams, however different they look, share the same underlying shape — an urgent, unexpected request for money, information, or secrecy, arriving through a channel the scammer controls. A plan built to answer that shape protects against nearly all of them at once, including brand-new ones, because it responds to what scams have in common rather than to their endless disguises.

This guide pulls the whole defense together into a simple, one-page playbook your family can adopt and keep by the phone. It gathers the handful of sturdy habits, the family safe word, the clear rules, and the key contacts into one place, so that any family member, young or old, confident with technology or not, has the same reliable response ready. We will walk through each piece, explain why it works, and then lay out the one-page playbook itself for you to copy and share. Simple, shared, and sturdy — that is the goal.

WATCH OUT

Don't try to memorize every scam — adopt one shared plan. It answers the shape all scams share, so it protects your family against today's cons and tomorrow's alike.

2. The Shape Every Scam Shares

What the plan is built to answer.

To see why one plan can cover so much, it helps to recognize the shape nearly every scam shares beneath its disguise. Whatever the story — a jailed grandchild, a bank fraud alert, a tax threat, a prize, a romance, a tech-support emergency, a too-good deal — the scam almost always needs the same few things from you. Learn to see that shape, and you stop having to identify which particular scam you are facing.

- An unexpected contact — a call, text, email, message, or pop-up you did not initiate.
- An urgent, pressing request — act now, there's no time, something terrible or wonderful will happen.
- A demand for money, personal information, account access, or secrecy.
- A channel the scammer controls, often with a faked voice, face, number, or sender.
- A push to avoid the very things that would expose it — checking, waiting, telling family.

When you look at scams this way, the endless variety collapses into one recognizable pattern. The grandchild-in-jail call and the fake-bank fraud alert and the too-good online deal are all the same shape wearing different costumes: an unexpected, urgent demand for money or information through a channel the scammer controls, with pressure to skip verification. Your family's plan is built to answer exactly that shape — to recognize it and respond the same safe way every time — which is why one plan can defeat so many different scams.

GOOD TO KNOW

Nearly every scam is the same shape in a different costume: an unexpected, urgent demand for money, info, or secrecy through a channel the scammer controls. Answer the shape, and you answer them all.

3. Habit One — Verify First

The core of the whole playbook.

The heart of the family playbook is a single habit: verify first. Before anyone acts on an urgent or unexpected request for money, information, or access, they confirm it through a separate channel they already trust — regardless of how the request arrived or how real it seems. Only after confirming do they act. This one habit is the backbone of the entire plan, and most of the other rules simply support it.

It works because it does not require spotting the fake, which AI has made nearly impossible. Scammers reach you through a channel they control and can make flawless; they cannot control a separate channel you choose and already trust. When you hang up and call your grandchild's real number, log into your bank the way you always do, or ask a question only the real person could answer, you step outside the scam entirely. A real request confirms itself on your trusted channel; a fake one cannot.

The two 'nevers' make verification genuine: never verify through the same channel that contacted you (the scammer controls it and will happily insist they are real), and never use a number, link, or contact the suspicious message provided (it leads back to them). Always reach the real party independently — a number from your card, your saved contacts, an app you installed, an official site you type yourself. Taught to the whole family, verify first is the single most protective habit there is, and I have a full guide devoted to it if you would like more.

WATCH OUT

Verify first means: confirm any urgent request on a SEPARATE channel you ALREADY trust — never the one that contacted you, and never a number or link it gave you.

4. Habit Two — Never Rushed, Never Secret

Refusing the scam's two engines.

The second habit targets the two feelings every scam needs to create: urgency and secrecy. So the rule is simple: about money, your family is never rushed and never secret. No one makes a money decision while being pressured to hurry, and no one keeps a money decision secret from the family. These two refusals, together, defeat an enormous range of scams, because they deny the scam the exact conditions it requires to work.

Urgency is manufactured to stop you from pausing to think or check. A real emergency survives a short pause; a real opportunity survives a day's thought; a real institution does not punish you for taking a moment. So when a request insists you must act this instant, that pressure is itself the warning sign, and the rule says: slow down precisely when you are pushed to hurry. Secrecy is manufactured to keep you isolated from the people who would recognize the scam. So when told to keep something quiet, the rule says: tell someone you trust, which is exactly what the scammer fears.

Taught as a family rule, 'never rushed, never secret' is remarkably powerful because it requires no scam-spotting at all. A family member does not have to figure out whether a request is legitimate; they simply refuse to be hurried and refuse to keep money matters secret, and those two refusals alone cause most scams to collapse. Pair this with verify first, and you have the core of a defense that holds against the grandchild scam, the bank-impersonation scam, the pressure scripts, and far more.

WATCH OUT

Urgency and secrecy are the two engines of nearly every scam. 'Never rushed, never secret' about money defeats them without you having to spot the scam at all.

5. Habit Three — The Family Safe Word

Your backup against faked voices and faces.

The third piece of the playbook is a family safe word — a private word or short phrase your family agrees on in advance, known only to you and an outsider could never guess, and that you would never post online. Its job is to verify a 'loved one in trouble' contact when you cannot reach the person another way: if a frightening call or message claims to be family and asks for money, you ask for the safe word. A real loved one knows it; a cloned voice, a deepfake, or an impostor does not.

The safe word is powerful precisely because it tests knowledge, which fakes lack, rather than appearance, which they can now mimic perfectly. Voice cloning can copy a grandchild's voice from seconds of audio, and deepfakes can fake a familiar face on a video call, so your ears and eyes are no longer proof. But none of those fakes can supply a private word they have never heard. The safe word is your sturdy backstop for exactly the moment the new technology is designed to beat.

Choosing one is a quick, even fun, family activity: pick something memorable but odd — a silly pairing of two unrelated words works beautifully — steer clear of anything guessable like a pet's name or a birth year, agree on it together, and say it aloud once so it sticks. Teach the rule alongside it: if someone in a panic about money cannot give the word, slow down and verify before doing anything. The safe word is a backstop to verify first, not a replacement, and I have a full workbook on choosing and using one if you would like it.

TIP

A family safe word tests knowledge a fake can't have. Pick something private and odd (not a pet's name or birth year), agree on it together, and say it aloud once so everyone remembers.

6. Habit Four — Know the Payment Red Flags

The methods that mean 'scam.'

The fourth piece of the playbook is knowing the payment methods that signal a scam, because how money is demanded is one of the clearest giveaways of all. Scammers steer you toward payments that are fast, reach them anywhere, and cannot be reversed, which is why the same handful of methods appears across nearly every scam. Teaching the family these red-flag methods gives everyone a simple, reliable alarm bell.

- Gift cards — being told to buy store cards and read the numbers over the phone. No legitimate institution does this.
- Wire transfers or money-transfer services to a name you don't know.
- Cryptocurrency, often through a machine at a store, with a caller coaching you.
- A courier sent to your door to collect cash, gold, or jewelry.
- Moving your money to a 'safe account' at someone's direction.

The rule is simple: the family never pays by any of these at the direction of a caller, a message, or anyone who contacted you. No real bank, court, government agency, utility, business, or charity collects money in gift cards, and legitimate emergencies and

purchases do not require wiring money to strangers or feeding cash into crypto machines. Any of these demands, by itself, is strong proof of a scam, no matter how convincing the story around it. Let the payment method be a bright, simple warning the whole family recognizes.

WATCH OUT

Gift cards, wire transfers, crypto, a cash courier, or 'move your money to a safe account' — any of these, demanded by a caller or message, is a scam. Make the family's answer an automatic no.

7. Habit Five — The Open Door

No judgment, so everyone speaks up.

The fifth and perhaps most important piece is the open door: an understanding that any family member can bring a worrying call, message, or decision to the family — or to one trusted person — for a sanity check, anytime, with absolutely no judgment, teasing, or scolding. This single agreement may protect your family more than any other, because scams depend on secrecy and shame, and an open door defeats both.

Here is why it matters so much. The reason people fall deep into scams, and the reason they lose the most, is often that they are too embarrassed to ask or too afraid of being lectured, so they handle it alone and in secret — exactly the isolation the scammer engineered. A family where it is completely safe, even normal, to say 'I got a strange call, does this sound right?' has a built-in second set of eyes on every scam, catching them early, while the money can still be saved and before shame sets in.

Making the door genuinely open takes a promise and then living up to it. Agree, out loud, that no one will ever be made to feel foolish for asking or for a close call, and that reaching out is always welcome and smart. Then honor it: the first time a family member brings you a worry or admits a mistake, your warm, grateful, non-judgmental response teaches everyone that the door is real. That safety to speak up, maintained over time, is the warm heart of the whole playbook and the protection that holds when all else is uncertain.

GOOD TO KNOW

Scams run on secrecy and shame. A family where anyone can ask 'does this sound right?' with zero judgment has a second set of eyes on every scam — and catches them while the money can still be saved.

8. The One-Page Playbook Itself

Everything on a single page to copy and post.

Here it is — the whole family's scam defense on one page, ready to copy out, print, or write on a card and keep by the phone and the computer. Read it together, fill in your family's specifics, and post it where everyone can see it. This single page, shared and understood, is the heart of protecting your family against today's scams and tomorrow's.

OUR FAMILY SCAM PLAYBOOK

- **VERIFY FIRST.** Any urgent request for money, information, or access, we confirm on a number or channel we already have — never the one that contacted us, never a number or link it gave us.
- **NEVER RUSHED, NEVER SECRET** about money. A real matter survives a pause; we tell each other.
- **OUR SAFE WORD** is: _____ (private, never posted). We ask for it on any 'loved one in trouble' call we can't otherwise verify.
- **NO GIFT CARDS, WIRES, CRYPTO, COURIERS,** or 'safe accounts' at anyone's direction. Our automatic answer is no.
- **THE SCREEN IS NOT PROOF.** Caller ID, a familiar voice, a familiar face, and a real-looking email can all be faked. We verify anyway.
- **THE DOOR IS OPEN.** Anyone can ask 'does this sound right?' anytime, no judgment, ever.

OUR TRUSTED CONTACTS

- Call first before acting: _____ and _____
- Our bank (real number from the card): _____
- Bill's Home Tech, local help: (330) 200-8042
- Report scams: [FTC ReportFraud.ftc.gov](https://www.ftc.gov/ftcr) · [FBI ic3.gov](https://www.fbi.gov) · Ohio AG 800-282-0515

TIP

Fill in the blanks with your family's safe word and 'call first' people, then post this page by the phone. A plan you can glance at beats memory in a frightening moment.

9. Setting It Up as a Family

A five-minute conversation.

The playbook only works if the whole family shares it, so the setup is a short, warm conversation rather than a lecture to one 'vulnerable' member. Pick a relaxed moment — a holiday, a Sunday dinner, a regular visit — and go through the page together, as equals, with everyone adopting the same habits. Framing it as 'this is just how our family handles this now' removes any sting and makes it a shared norm rather than a worry aimed at anyone.

In that conversation, do the concrete things: choose your family safe word and say it aloud once; fill in the 'call first' people and the key numbers; make sure everyone has each other's real numbers saved; and make the open-door promise out loud, together. Keep the tone light and collaborative. Let the grandchildren help the grandparents with the technology pieces while the grandparents share why it all matters; both generations come away better protected, and the whole thing feels like togetherness, not supervision.

Then make it real and lasting: write the playbook on cards or print it, post it by the phones and computers in the house, and revisit it lightly now and then — mentioning a scam in the news, sharing a strange call you got. A plan set up once and never spoken of again fades; a plan that lives in a visible card and an occasional friendly chat stays ready. Five minutes to set it up, a glance now and then to keep it fresh, and your family carries a defense that covers nearly everything.

WATCH OUT

Set it up at a relaxed family moment as 'how our family does this now,' not a warning to anyone. Choose the safe word, fill in the contacts, make the open-door promise — all together.

10. The Playbook Against the Grandchild Scam

Seeing the plan in action.

It helps to see how the one-page playbook handles specific scams, so the family trusts that it really works. Take the cloned-voice grandchild scam: a call comes, a voice just like your grandchild sobs that they are in jail and need bail money now, and a 'lawyer' demands gift cards and secrecy. It is frightening and convincing. Now watch the playbook answer it, line by line, without anyone needing to 'spot' anything.

'The screen is not proof' and the knowledge that voices can be cloned mean you do not trust the voice, however real it sounds. 'Verify first' means you hang up and call the grandchild's real number, or their parents. 'Never rushed, never secret' means the urgency and the 'don't tell anyone' are warning signs, not instructions. 'No gift cards' means the payment demand is an automatic no. And the 'safe word' is ready as a backstop if you cannot reach the grandchild directly. Every single element of the scam runs straight into a line of your playbook and stops.

Notice that at no point did anyone have to recognize 'this is the cloned-voice grandchild scam.' The playbook handled it just by being applied to the shape of the request — urgent, secret, odd payment, a voice that can't be trusted. That is the beauty of the one-plan approach: your family defeats a sophisticated, frightening, AI-powered scam simply by following their shared habits, with no scam-spotting expertise required. The same walkthrough works for the bank scam, the government scam, the romance scam, and the rest.

GOOD TO KNOW

Against the cloned-voice grandchild scam, every element — the fake voice, the urgency, the secrecy, the gift cards — runs straight into a line of the playbook and stops. No scam-spotting required.

11. The Playbook Against Impersonation

Bank, government, and tech-support calls.

The playbook handles impersonation scams — the fake bank fraud alert, the fake IRS or Social Security threat, the fake tech-support pop-up — just as cleanly. In each, someone claims to be a trusted institution, your screen may show the real name or number, and you are pressured to pay, share information, or grant access urgently. The costumes differ, but the shape is the same, and the playbook answers it the same way.

'The screen is not proof' means a convincing voice and a correct-looking caller ID or email prove nothing, because all can be faked. 'Verify first' means you hang up and reach the bank on the number from your card, or the agency through its official site, or the company through a channel you chose — never a number the caller or pop-up gave you. 'Never rushed, never secret' meets the manufactured urgency and any demand for quiet. 'No gift cards or safe accounts' stops the payment. And the open door means you can check it with family before acting.

Again, no one had to diagnose exactly which impersonation it was. Whether it claimed to be the bank, the IRS, the sheriff, or Microsoft support, the family applied the same habits to the same shape and the scam collapsed. This is why the one-page playbook is so much more practical than a scam-by-scam education: a family that truly holds these few habits is protected against the whole sprawling family of impersonation scams, and against the new variations that will keep appearing, all with one simple, shared response.

GOOD TO KNOW

Bank, IRS, sheriff, or 'Microsoft' — impersonation scams all meet the same playbook: the screen isn't proof, verify first on a channel you chose, and no gift cards. One response, every disguise.

12. The Playbook Against Online Scams

Phishing, fake stores, and investment cons.

The playbook extends naturally to the online scams too — phishing emails and texts, fake stores and reviews, deepfake investment pitches, romance and pig-butcherer cons. These reach you through your inbox, your feed, and your screen rather than a phone call, but they share the same shape, and the same habits answer them with small, sensible extensions for the online world.

'Verify first' becomes: don't act through the message — reach the company, bank, or person through a channel you already trust (their app, your bookmark, a known number). 'The screen is not proof' covers flawless fake emails, fake stores, fake reviews, and deepfake videos alike. 'Never rushed, never secret' meets the countdown timers and 'act now' pressure. 'No gift cards, wire, or crypto' and a preference for paying by credit card handle the money side. And for anything that found you — an unexpected email, an ad, an online 'friend' turning to money — the family's instinct is caution and independent verification.

For the relationship-based online scams especially, one playbook extension is worth stating: the family never moves money or invests because of someone met online, and never lets a screen alone move money. With that, the romance scams, the pig-butcherer investment cons, and the deepfake video-call frauds all meet the plan and stop. Across phone, inbox, feed, and screen, the one-page playbook — verify first, never rushed or secret, the screen isn't proof, no odd payments, the open door — covers the whole modern landscape of scams with a single, shared, sturdy response.

GOOD TO KNOW

Online, verify first means 'don't act through the message — reach them your own way,' and the family never moves money for someone met online. The same plan covers inbox, feed, and screen.

13. Teaching Every Generation

The plan is for young and old alike.

A key strength of the family playbook is that it is for everyone, not just the oldest members, and teaching it across the generations makes the whole family a seamless defense.

Scams target every age — grandparents with the jailed-grandchild call, parents with the impostor-child text, young people with job, gaming, romance, and account-takeover scams — and the AI fakes fool the young and tech-savvy as readily as anyone. A plan held only by some leaves gaps the scammers find.

So teach the playbook to children and grandchildren as a life skill, framed as savvy rather than fearful: you don't have to be suspicious of everyone, you just verify anything important before acting. Connect it to what they care about — protecting their own accounts and money, and protecting the grandparents they love, whose voices could be cloned from the family's own videos. Make it a two-way exchange, with the young teaching the old about new apps and the old sharing why the habits matter.

When every generation shares the same playbook, something powerful happens: there is no weak link for a scam to exploit, and the family becomes a mutual protection network. A grandchild can instantly confirm 'yes that's my new number' or 'no, I didn't call you' when a grandparent checks; a parent and an adult child apply the same rules; and everyone knows the safe word and the open-door promise. A whole family moving in step on one simple plan is remarkably hard to scam, in every direction across the generations.

TIP

Teach the playbook to the grandkids too, as a savvy life skill. When every generation shares it, there's no weak link — and the family becomes a mutual protection network.

14. Keeping the Plan Alive

A living habit, not a one-time talk.

A plan set up once and then forgotten slowly fades, so the final piece is keeping it alive with light, occasional touches rather than treating it as a single talk to get through. Scams evolve, memories dim, and new family members and devices come along, so the playbook stays strongest when it remains a gentle, ongoing part of family life rather than a dusty card no one looks at anymore.

Keeping it alive is easy and even pleasant. When a scam makes the news, mention it casually — 'did you hear about this one? Good thing we've got our plan.' When you get a strange call or a phishing text, share it with the family as a small story. Glance at the playbook card now and then and check that the contacts and safe word are current. These little touches reinforce the habits, keep the open door warm, and treat scam safety as a normal, shared part of looking out for each other.

Above all, keep proving the open door, because that is the piece that most needs tending. Every time a family member brings you a worry or a close call and you respond with warmth and gratitude rather than judgment, you deepen the trust that makes the whole plan work in the moment it matters most. A living playbook, revisited lightly and backed by a genuinely open door, gives your family a durable defense that keeps protecting them year after year, against whatever the scammers try next.

WATCH OUT

Keep the plan alive with light touches — share scam news and strange calls, check the card's still current. And keep proving the open door; that's the piece that matters most in the moment.

15. When a Scam Gets Through Anyway

The plan includes how to respond.

No defense is perfect, and part of a good playbook is knowing what to do if a scam gets through anyway, so a mistake becomes a manageable event rather than a catastrophe. If a family member realizes they have been scammed — sent money, shared information, or granted access — the plan kicks in with a calm, fast response, and above all with compassion rather than blame.

- 1 Lead with 'I'm so glad you told me — this is not your fault,' because shame keeps people from acting and asking for help.
- 2 Stop all contact with the scammer immediately.
- 3 Call the bank, card company, or payment provider right away to try to stop or reverse money; speed helps.
- 4 Change passwords and secure any accounts or devices that were exposed; turn on a second lock.
- 5 Save the evidence, tell the family, and report it (FTC, FBI for larger losses, Ohio AG).
- 6 Watch for the follow-up 'recovery' scam, and never pay anyone offering to get your money back.

The compassion matters as much as the steps. A family member who is met with warmth and help, rather than 'how could you,' will act quickly and will keep trusting the open door for next time. One who is shamed may hide the next scam, which is far more dangerous. So the playbook's response to a scam getting through is the same spirit as the rest of it: calm, together, and without judgment. I have a full guide on exactly what to do in the first thirty minutes after a scam if you would like the detail.

GOOD TO KNOW

If a scam gets through, lead with 'I'm so glad you told me — not your fault,' then act fast. Compassion keeps the family member trusting the open door, which protects them next time.

16. The Devices Part of the Plan

Setup that backs up the habits.

The habits are the heart of the playbook, but a few device setups quietly back them up, making your family safer by default even in a moment of inattention. These are one-time jobs, and they pair naturally with the habits to form a complete defense. If any feel fiddly, they are exactly the kind of thing I am glad to help a family with.

- Turn on spam-call filtering and consider 'silence unknown callers' so many scam calls never get through.
- Put a second lock (two-step verification) on email and banking — email especially, since it's the master key.
- Make sure everyone's important contacts are saved, so verifying callbacks are quick.
- Keep devices updated, which patches the holes scams exploit.
- Make a credit card the default for online shopping, for its strong protection.

None of this makes the technology harder to enjoy; it simply makes it safer underneath. Spam filtering stops many scam calls before they ring; the second lock protects accounts even if a password leaks; saved contacts make the verify-first habit effortless; updates close known weaknesses. Together with the habits on the playbook card, these setups give your family both a sturdy mindset and a safer set of devices, which is the strongest combination of all.

TIP

Back the habits with a little setup: spam-call filtering, a second lock on email and banking, saved contacts, and a credit card for online shopping. One-time jobs that protect every day.

17. A Note for Those Who Live Alone

Building the plan into a solo life.

The playbook is framed around a family, but its spirit applies just as much to someone who lives alone, with a small adaptation. Living alone removes the built-in second set of eyes that catches so many scams, and scammers target solo older adults heavily for exactly that reason. So the key is to deliberately build that second set of eyes back into your life, so you are not facing scams entirely on your own.

Name your people in advance: one or two trusted family members, friends, or neighbors you commit to calling before acting on any urgent money request, plus your bank's real number, and keep that short list right on your playbook card by the phone. Tell those people ahead of time that you may call with 'does this sound right?' questions, so they expect and welcome it. A safe word still works for verifying a 'loved one in trouble' contact, and a trusted person can be your sounding board whenever something feels off.

The rest of the playbook applies unchanged — verify first, never rushed or secret, the payment red flags, the screen isn't proof — and the device setups matter even more when there is no one else in the house to notice a problem. And please remember you can always add me to your short list: there is no charge to talk through a worrying call, and no judgment. Living alone does not mean facing scams alone, as long as you build your own second set of eyes into the plan in advance.

TIP

If you live alone, name one or two 'call first' people in advance and put them on your playbook card. Deciding who to check with, before the pressure comes, rebuilds the second set of eyes scams rely on your not having.

18. Why This Protects Against Tomorrow

A plan that doesn't go out of date.

One of the greatest strengths of the one-page playbook is that it does not go out of date. New scams and new technologies appear constantly — voice cloning and deepfake video calls were science fiction not long ago — and no list of specific scams can keep up. But the playbook is built on the shape all scams share and the habits that answer that shape, so it works against a brand-new scam just as well as a familiar one. Your family does not have to be re-taught with every new fraud.

Whatever scammers invent next, it will almost certainly still need to make an urgent, unexpected request for money, information, or access, through a channel it controls, while discouraging you from checking. And the playbook will still answer it the same way: verify first on a channel you trust, refuse urgency and secrecy, recognize the payment red flags, remember the screen isn't proof, and keep the open door. The disguises will change; the plan that defeats them will not. That durability is worth more than any amount of scam-by-scam knowledge.

So a family that truly adopts this one-page playbook is protected not just against today's scams but against the ones not yet invented, which is a remarkable thing to be able to say. You cannot predict the next fraud, but you do not need to, because you have a response ready for the shape all of them share. Set up the plan, keep it alive, hold the open door, and your family carries a defense that will keep serving them for years, through whatever comes next.

GOOD TO KNOW

The playbook never goes out of date, because it answers the shape all scams share, not their disguises. A family that adopts it is protected against today's scams and the ones not yet invented.

19. Questions People Ask Me

The ones families bring to me most.

Isn't a one-page plan too simple to cover so many scams? Its simplicity is its strength. Because nearly all scams share one shape — an urgent, unexpected demand for money, info, or secrecy through a channel the scammer controls — a plan that answers that shape covers them all, including new ones. A long, complicated plan no one remembers protects far less than a simple one everyone follows.

My family member resists 'being told' what to do — how do I introduce it? Frame it as a shared family plan everyone adopts together, not advice aimed at them. 'Let's all set up some simple habits' lands far better than 'you need to be careful.' When the whole family, including the grandkids, takes it on equally, no one feels singled out, and resistance usually fades.

What's the single most important part if I can only do a little? The open door — making it completely safe to ask 'does this sound right?' with no judgment — plus 'verify first.' A family member who will check a worrying request with someone they trust, and who confirms before acting, is protected against most scams even without the rest.

Where do I get help setting up the pieces — the safe word, the device settings, the contacts? You can do it yourselves with this guide, or call me. Setting up a family's scam defense — the habits, the safe word, the spam filtering, the account locks, the saved contacts — is some of the most satisfying work I do, and I'm glad to walk any family through all of it, patiently and with no rush.

20. Your Playbook, in Five Minutes

Put it all in place today.

Here is how to put the whole playbook in place for your family in about five minutes, so you leave this guide with a real, working defense rather than just good intentions. Do it together, keep it light, and you will have given your family protection against today's scams and tomorrow's alike.

- 1 Read the one-page playbook together and agree to adopt it as 'how our family does this.'
- 2 Choose your family safe word — private, odd, never posted — and say it aloud once.
- 3 Fill in your 'call first' people, your bank's real number, and the report contacts.
- 4 Make sure everyone has each other's real numbers saved in their phones.

- 5 Make the open-door promise out loud: anyone can ask anytime, no judgment.
- 6 Write or print the playbook on cards, post them by the phones, and revisit lightly now and then.

GOOD TO KNOW

If you do just two things, make them the open-door promise and 'verify first.' A family that asks before acting and confirms on a trusted channel is remarkably hard to scam.

21. Reporting It — and Why It Helps

A few minutes that protect the next person.

Reporting a scam can feel pointless once the money is gone, but it genuinely matters. Reports help investigators link cases together, give platforms and phone carriers the evidence to shut fakes down, and warn others before they are caught. You do not need to have lost money to report — flagging an attempt is valuable too. It takes only a few minutes, and it turns a bad experience into something that helps your neighbors.

- Report to the Federal Trade Commission at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov), the national clearinghouse for scams. You can also call 1-877-382-4357.
- Report online or financial crime to the FBI at ic3.gov, their internet-crime complaint center — especially for larger losses or cryptocurrency.
- Contact the Ohio Attorney General's consumer protection team at 800-282-0515 or through ohioattorneygeneral.gov.
- If your identity may be exposed, visit IdentityTheft.gov for a step-by-step recovery plan.
- Report spam texts by forwarding them to 7726 (SPAM), and use the 'report' button inside apps and email.

I wrote a separate, step-by-step guide on reporting to the FTC, the FBI, and the Ohio Attorney General, with exactly what to write down and what to expect afterward. If the reporting steps feel like a lot, that is a perfect thing to call me about. I am glad to sit with you and help you file, so that your report actually reaches the people who can use it.

GOOD TO KNOW

You will usually not hear back from a report, and that is normal. Your report still joins a bigger picture that helps investigators and warns others, even when nothing lands in your own inbox.

22. When to Just Call Me

A calm second opinion costs you nothing.

If something about setting up one simple scam-defense plan for your whole family has you second-guessing yourself, or you just want a steady second opinion before you do anything, please call me. There is never a charge to ask a scam question, and never any judgment. I would far rather spend a few minutes on the phone talking it through with you than hear later that something cost you money or worry. That is genuinely what I am here for, and it is some of the most satisfying work I do.

If you would like a hand in person, I come to homes all across Portage County. I can help you check something safely, tighten up your accounts and passwords after a close call, set your devices and routine so these scams have a harder time reaching you, and walk your whole family through a simple plan. We go at your pace, with no pressure and no rushing, and you come away feeling steadier.

GOOD TO KNOW

The best time to call is before you act — before you click, pay, or share anything. A quick 'does this seem right to you, Bill?' is one of my favorite kinds of call to get.

23. Contact Card & a Warm Close

Keep this page where you can find it again.

Bill's Home Tech — your local tech, Bill Davis, owner and only tech. Phone or text: (330) 200-8042. Email: bill@billshometech.com. Web: billshometech.com. Service area: Atwater, Ravenna, Kent, Streetsboro, Aurora, Rootstown, Mantua, Garrettsville, Windham, Edinburg, Suffield — all of Portage County, Ohio.

- Free phone call: any scam question or close call, always free, with no judgment and no rushing.
- In-home scam-check visit: \$99 flat for the first visit, with a 30-day follow-up included.
- Remote help by screen-share, for when you would rather not wait for a visit.

One simple plan, shared by the whole family, beats a hundred separate worries. Set it up together, keep it by the phone, and call me anytime you'd like help putting any piece of it in place. I am a phone call away, and glad to help your whole family stay safe.

CHEAT SHEET

The One-Page Playbook

Our family habits

- VERIFY FIRST — confirm urgent requests on a number we already have.
- NEVER RUSHED, NEVER SECRET about money.
- SAFE WORD: _____ (private, never posted).
- NO gift cards, wire, crypto, couriers, or 'safe accounts.'
- THE SCREEN ISN'T PROOF — voice, face, caller ID, email can all be faked.
- THE DOOR IS OPEN — anyone can ask 'does this sound right?', no judgment.

Our contacts

- Call first: _____ and _____
- Our bank (from the card): _____
- Bill's Home Tech: (330) 200-8042
- Report: FTC ReportFraud.ftc.gov · FBI ic3.gov · Ohio AG 800-282-0515

If a scam gets through

- 1 'I'm so glad you told me — not your fault.'
- 2 Stop contact; call the bank/card right away.
- 3 Change passwords; turn on a second lock.
- 4 Save evidence; tell the family; report it.
- 5 Ignore any 'recovery' offer for a fee.

GOOD TO KNOW

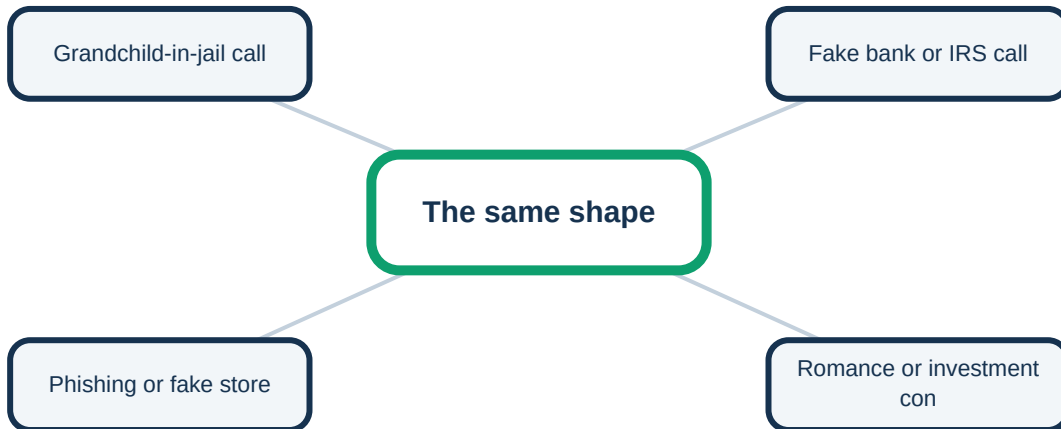
One shared plan beats a hundred memorized scams — it answers the shape they share, so it protects against today's cons and tomorrow's. Keep it by the phone.

AT A GLANCE

A Picture to Follow Along

One Plan, Every Scam

They all share a shape the playbook answers.



Urgent + secret + odd payment - answer the shape, beat them all.

Illustration - a schematic; details vary by device and setup.

AT A GLANCE

A Second Look

The Family Playbook

Six habits, on one page, by the phone.

- 1 Verify first - confirm on a number you already have
- 2 Never rushed, never secret about money
- 3 Use the family safe word for 'loved one' calls
- 4 No gift cards, wire, crypto, or 'safe accounts'
- 5 The screen isn't proof - voice, face, ID can be faked
- 6 The door is open - ask anytime, no judgment

One shared plan protects against today's scams and tomorrow's.

Illustration - a schematic; details vary by device and setup.

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.