



Lock Down Your Own Voice — Making Family Videos Private on Facebook, Instagram & TikTok

Making your videos and voice private — one simple setting at a time.

————— **An Extended Guide · No. 1625 · 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 I Wrote This One	4
2. Why Your Voice Is Worth Protecting	5
3. The One Setting That Matters Most	6
4. Facebook — Setting Your Audience	6
5. Instagram — Switching to Private	7
6. TikTok — Private Account and Downloads	8
7. YouTube — Public, Unlisted, or Private	9
8. Your Voicemail Greeting	9
9. The Other Places Your Voice Lives	10
10. Helping the Grandkids Lock Down Too	11
11. Stories and Disappearing Posts	12
12. When Other People Post You	12
13. Public Pages and Business Accounts	13
14. Checking Your App Permissions	14
15. A Word on Smart Speakers	15
16. Keeping Settings From Drifting	15
17. A Word on Face and Photos	16
18. What Settings Can't Do	17
19. The Callback Habit, One More Time	18
20. A Gentle Settings Checklist	18

21. Questions People Ask Me	19
22. A Five-Minute Family Privacy Setup	20
23. Reporting It — and Why It Helps	20
24. When to Just Call Me	21
25. Contact Card & a Warm Close	22
Everyday Cheat Sheet	22
A Picture to Follow Along	24
A Second Look	25
A Note From Bill	25
Your Visit — and My Promise	26

SUMMARY

The 60-Second Version

A scammer needs only a few seconds of recorded speech to copy a voice, and most of us have more than that sitting in public on social media. You don't have to stop sharing — you just set your talking videos to friends-only, keep a plain voicemail greeting, and remind the grandkids their public clips can be grabbed too. A few minutes of settings make it much harder for a stranger to steal your voice or your face.

- 1 Set your social accounts and videos to friends-only or private, not public.
- 2 Keep your voicemail greeting plain, or use the phone's default robot voice.
- 3 Think twice before posting long talking videos to public accounts.
- 4 Check who can see your old posts, and tighten the public ones.
- 5 Ask grandkids to set their talking videos private too — their voice matters.

GOOD TO KNOW

This is a bonus layer, not your main defense. The habit that truly protects you is the callback: a voice is never proof, so always verify by calling back on a known number. Settings just make you a harder target.

1. Why I Wrote This One

A few easy settings make you a harder target.

In more than thirty years of helping folks around Portage County with their devices, I have learned that most people want to protect themselves online but feel lost in the tangle of settings. This guide is my attempt to make one worthwhile corner of that simpler. Because scammers can now copy a familiar voice from just a few seconds of recorded speech, it is worth spending a few quiet minutes making your videos and your voice harder to grab. Not to hide from the world — just to close the easy doors.

I want to be honest right up front about what this does and does not do. Tightening your privacy settings is a good, sensible layer of protection, and I will walk you through it gently. But it is not your main defense against voice-cloning scams, and I would never want you to think that a locked-down account means you are safe to trust any voice on the phone. The real protection is the callback habit, which I will come back to. Think of settings as locking the windows, and the callback as never opening the door to a stranger.

We will go app by app — Facebook, Instagram, TikTok, YouTube — plus your voicemail greeting and a few other quiet sources of your voice. The exact wording of menus changes

from time to time and differs a little between phones, so I will describe what you are looking for in plain terms rather than promising the buttons will be labeled exactly so. And if any of it gets fiddly, that is precisely the kind of thing I am glad to sit down and help with.

WATCH OUT

You do not have to do all of this at once. Pick one app today, tighten it, and feel good about it. You can do the next one next week. Progress beats perfection every time.

2. Why Your Voice Is Worth Protecting

A few seconds of sound is all it takes.

It helps to understand exactly why this is worth a few minutes of your time. Modern tools can copy the sound of a specific person's voice from a surprisingly short sample — consumer-protection officials and news tests put it at anywhere from a few seconds to around twenty. Feed a program that sample, and it can then make your voice say anything. Scammers use this to call your loved ones pretending to be you, or to make a cloned voice of your grandchild to call you.

The raw material for that theft is usually not a secretly recorded phone call. It is the ordinary speech we post without a second thought: a chatty video to the grandkids, a clip of you singing in the church choir, a welcome video for a small business, a long voicemail greeting. Any of these, if public, hands a stranger a clean sample of your voice. The clip you thought was just a sweet moment can become the ingredient in a scam aimed at someone you love.

None of this means your memories are dangerous or that you should stop sharing life online. It means the material is out there for most families, so it is smart to reduce how much of it sits wide open to strangers. Making your talking videos visible only to friends, rather than to the entire internet, dramatically shrinks the pool a scammer can fish in — without costing you the joy of sharing with the people who actually matter to you.

GOOD TO KNOW

Even a private account is not a vault — a friend can reshare your clip, and settings can reset after an app update. That is why settings are a helpful layer, not a guarantee, and the callback habit still matters most.

3. The One Setting That Matters Most

Public versus friends-only, everywhere.

If you remember just one idea from this whole guide, make it this: the single most valuable setting on any app is the one that controls who can see what you post. Nearly every platform offers some version of a choice between 'public' — meaning anyone in the world, including strangers and scammers — and 'friends only' or 'private,' meaning only people you have approved. Shifting from public to friends-only is the one change that does the most good, on every app.

This matters because a public account is an open invitation. Any video, photo, or voice clip you post publicly can be viewed, downloaded, and reused by anyone, with no way for you to know it happened. A friends-only account limits that audience to people you have chosen, which is almost certainly who you wanted to share with in the first place. For most of us, friends-only loses nothing we actually care about and closes a wide-open door.

There are two layers to this on most apps, and both are worth setting. First, there is often an account-wide setting that makes everything you post default to a chosen audience. Second, each individual post usually has its own audience setting you can check and change. The account-wide setting is the big win; the per-post setting is useful for old public posts and for anything you want to share more widely on purpose. We will hit both as we go app by app.

TIP

When in doubt on any app, look for words like 'Who can see this,' 'Audience,' 'Privacy,' or a globe icon (which means public). Changing a globe to 'Friends' is the move you are looking for almost everywhere.

4. Facebook — Setting Your Audience

The most common home for family videos.

Facebook is where most families share, so it is worth starting here. Facebook gives you a setting that controls who can see your future posts, and separate tools to limit who can see your past posts. You reach these through the menu (often three lines or your picture), then Settings & Privacy, then Settings, then the privacy section. Because Facebook rearranges its menus from time to time, look for the ideas rather than exact labels: 'Who can see your future posts,' 'Limit past posts,' and 'How people find and contact you.'

- Set 'Who can see your future posts' to Friends, so new posts are not public by default.
- Use 'Limit who can see past posts' (sometimes called 'Limit past posts') to make old public posts Friends-only in one step.
- Review 'Who can see your friends list' and your profile details, and tighten those to Friends.
- Turn off or limit 'Do you want search engines outside Facebook to link to your profile.'
- For any single post, use the audience button (near the Post button) to set it to Friends before sharing a video.

The 'Limit past posts' tool is especially handy, because it sweeps up years of old public posts at once rather than making you fix each one. After you have set future posts to Friends and limited the past ones, your Facebook is in much better shape. If the menus look different on your phone than on a computer, the same options are usually there under Settings and Privacy — just in a slightly different order.

WATCH OUT

Even on Friends-only, remember that a friend can share your video to their own audience, which may be public. Be a little thoughtful about talking videos even among friends, and ask relatives not to reshare yours publicly.

5. Instagram — Switching to Private

One switch does most of the work.

Instagram makes this refreshingly simple with a single, powerful switch: you can set your whole account to Private. When your account is private, only people you approve as followers can see your photos, videos, and stories; strangers cannot. For most people, especially those sharing family moments rather than running a public page, flipping to Private is the right choice and takes less than a minute.

You find it by opening your profile, tapping the menu (often three lines in the corner), going to Settings and privacy, then 'Account privacy,' and turning on 'Private account.' Once it is on, anyone who wants to follow you has to send a request you approve, which puts you back in control of who sees your voice and face. Existing followers stay, so you are not cutting off the family you already share with.

A couple of notes help. If you have been public and had strangers following you, switching to private is a good moment to review your followers and remove any you do not recognize. And remember that even on a private account, anyone you approve can still screenshot or

re-record what you post, so private is a strong layer rather than an absolute lock. For family sharing, though, it is exactly the right setting, and I recommend it to nearly everyone.

WATCH OUT

After switching to Private, scroll through your follower list and remove anyone you do not actually know. A clean follower list means your private posts really are reaching only people you trust.

6. TikTok — Private Account and Downloads

Where the grandkids often are.

TikTok is built around short videos and is especially popular with younger family members, which makes it a common source of clean voice clips. Like Instagram, it offers a private-account switch, plus a few extra settings worth turning off because they specifically control whether others can grab your videos. If you or a grandchild post talking videos here, these settings are well worth a look.

- Open your profile, go to the menu, then Settings and privacy, then Privacy, and turn on 'Private account.'
- Turn off 'Allow your videos to be downloaded,' so viewers cannot save your clips to their own devices.
- Limit who can Duet, Stitch, or comment on your videos to Friends or No one.
- Turn off 'Suggest your account to others' so strangers are not nudged toward you.
- Review and remove followers you do not recognize after going private.

The download setting is the one people overlook, and it matters here: even a thoughtful post can be saved by a stranger if downloads are allowed. Turning downloads off, along with setting the account private, closes the easiest ways for someone to walk off with a copy of your voice and face. If a grandchild loves TikTok and will not go private, at least ask them to turn off downloads and to think about talking videos.

WATCH OUT

Short, temporary-feeling videos are just as grabbable as any other. 'It's only up for a day' is no protection if downloads are on or the account is public.

7. YouTube — Public, Unlisted, or Private

Three choices, and what each means.

YouTube handles this a little differently, giving each video one of three visibility settings rather than one account-wide switch. Understanding the three choices lets you share a family video with just the people you want. The three are Public (anyone can find and watch it), Unlisted (only people with the link can watch, and it does not show up in search), and Private (only specific people you invite can watch).

- Public: anyone in the world can find and watch — avoid this for family and talking videos.
- Unlisted: only people you send the link to can watch; good for sharing a family video without putting it in search.
- Private: only specific Google accounts you invite can watch; the tightest option for sensitive clips.
- You set this when you upload, and you can change it later under your videos in YouTube Studio or your account's content list.

For most family sharing, Unlisted is the sweet spot: you can send grandma the link to the grandkids' recital without broadcasting it to the world or feeding it into search results where a stranger might stumble on it. For anything more sensitive, Private is tighter still. The key move is simply to stop posting family and talking videos as Public, and to go back and change any old Public ones to Unlisted or Private.

TIP

Go through your existing YouTube uploads and switch any family or talking videos from Public to Unlisted. It is a quick change per video and takes them out of public search.

8. Your Voicemail Greeting

A quiet source of your voice you may have forgotten.

Here is a source of your voice that almost everyone forgets: your voicemail greeting. If your greeting is a recording of you speaking — 'Hi, you've reached Mary, I can't come to the phone right now' — then anyone who calls your number and lets it ring to voicemail hears, and can record, a clean sample of your actual voice. Scammers sometimes call numbers for exactly this reason, to harvest the greeting.

The simple fix is to use your phone's default, automated greeting instead of your own recorded voice. The default greeting is usually a robotic voice that just reads back your

number, which gives a caller nothing of your voice to steal. You lose a little personal touch, but you close a door that most people never realized was open. On most phones you change this in the Phone app's voicemail section, or your carrier can switch it for you.

If you prefer to keep a personal greeting, at least keep it very short and plain — a sentence is plenty. The longer and more expressive the greeting, the better the sample it provides. But honestly, switching to the default robot greeting is the cleaner choice, and it is the kind of small change that costs you almost nothing while quietly removing one of the easiest ways for a stranger to grab your voice.

GOOD TO KNOW

Switching to the phone's default voicemail greeting is one of the single easiest privacy wins there is. Callers who reach voicemail hear a robot, not you, and have nothing to copy.

9. The Other Places Your Voice Lives

Beyond social media and voicemail.

Social media and voicemail are the big sources, but your voice can live in other public places too, and it is worth a quick mental inventory. The goal is not to track down and erase every trace — that is neither possible nor necessary — but to be aware of the main ones so you can tighten what is easy and be a little thoughtful about the rest.

- Recorded sermons, talks, lectures, or meetings that get posted online by a church, club, or organization.
- Podcasts or interviews you have taken part in, which often stay online for years.
- Webinars, online classes, or video calls that were recorded and shared.
- Business welcome videos, voicemail systems, or 'about us' pages that feature your voice.
- Videos friends or relatives posted that include you talking, even if your own accounts are private.

For the ones you control, the same ideas apply: ask whether it needs to be fully public, and tighten it if not. For the ones others control — a church recording, a friend's post — you can politely ask the person or organization to limit the audience or remove an old clip if it concerns you. Most will happily oblige once you explain why. And for the rest, simply knowing they exist helps you keep the right mindset: your voice is partly public, so your real safety rests on the callback habit, not on secrecy.

WATCH OUT

If a club, church, or business posts recordings of you, a friendly word is often enough to get an old clip limited or removed. It never hurts to ask.

10. Helping the Grandkids Lock Down Too

Their voices can be used against you.

This is not only about your own voice. A cloned voice of a grandchild is exactly what scammers use to call you with a fake emergency, so helping the younger family members tighten their accounts protects everyone. Younger people often post the most talking videos and often assume privacy does not matter to them, so a gentle conversation can do real good without turning into a lecture.

Rather than telling them to lock everything down, explain the why in a way that lands: their public talking videos could be used by a scammer to make a fake call to grandma, pretending to be them in trouble. Framed that way, as protecting the people they love rather than restricting themselves, most young people take it seriously and are often happy to flip their accounts to private, or at least to turn off downloads and think twice about long talking clips.

Make it a two-way exchange. Let the grandkids show you how the newest app's settings work — they usually know, and they enjoy being the teacher — while you share why it matters. A family where everyone, young and old, keeps their talking videos reasonably private is a family that gives scammers much less to work with, in every direction across the generations.

GOOD TO KNOW

Tell grandkids plainly: a public talking video of you could be used to fake a call to Grandma. That reason tends to land far better than 'be careful online.'

11. Stories and Disappearing Posts

'Temporary' doesn't mean safe.

Many apps have 'stories' or disappearing posts that vanish after a day, and they can lull you into sharing more freely because they feel fleeting. In truth, a story is just as grabbable as any other post while it is up. Anyone who can see it can screenshot it or record it, and if your account is public, that means anyone at all. The sense that it will soon be gone is a feeling, not a protection.

So apply the same thinking to stories that you apply to regular posts. If your account is private or friends-only, your stories are limited to that audience, which is the main win. Most apps also let you control who sees your stories specifically, sometimes with a 'close friends' option for the most personal ones. It is worth setting that so your talking stories reach only the people you truly mean to share them with.

The same caution applies to live video, which some apps offer. Going live publicly broadcasts your voice and face to anyone watching, and the recording may remain afterward. If you enjoy going live with family news, do it on a private account or to a limited audience. The joy of sharing in the moment is real, and you can keep it while still not broadcasting yourself to the whole internet.

WATCH OUT

'It disappears in 24 hours' is no protection. While it's up, a story can be saved by anyone who sees it — so the account's privacy setting is what really matters.

12. When Other People Post You

Tags, shares, and photos you didn't take.

You can lock down your own accounts perfectly and still appear, voice and face, in posts made by others — a friend's video of a dinner, a club's event recap, a relative resharing your clip to their public page. You cannot control other people's settings, but you have more influence than you might think, and a few gentle habits reduce how often you turn up in public through someone else's account.

Most apps let you control tagging: whether others can tag you, and whether tagged posts appear on your profile without your review. Turning on a setting that lets you review tags before they attach to you is worth doing. Beyond settings, a simple, friendly request goes a

long way: ask family and friends not to post talking videos of you publicly, and to set such clips to friends-only. Most people happily agree once you explain you are trying to keep your voice out of scammers' reach.

If a public post of you already exists and concerns you, you can usually ask the person to limit its audience or take it down, and most will oblige. For organizations like a church or club, a polite note to whoever manages their page is often all it takes. You will not catch every instance, and that is fine — the aim is to reduce the easy, public exposure, not to achieve the impossible task of erasing yourself from every friend's phone.

TIP

Turn on tag review if your apps offer it, and ask relatives to keep talking videos of you friends-only. A kind word to family does more than any single setting.

13. Public Pages and Business Accounts

When you need to be public on purpose.

Some people need a public presence — a small-business page, a ministry, a community group, an artist or author sharing work. If that is you, going fully private is not practical, and that is perfectly reasonable. The goal shifts from hiding to being thoughtful about which parts of you are public, keeping your personal voice and family life separate from your public-facing material.

A good approach is to keep two clearly separate things: a public page or account for your business or role, and a private personal account for family and friends. On the public side, you can share your products, services, and messages while being deliberate about how much clear, personal talking video of yourself you post, since that is the raw material for a voice clone. A business welcome video is fine; just know it is public, and keep the personal family clips on the private side.

It is also worth being aware that a public business presence makes you a more visible target for impersonation — scammers sometimes clone a business owner's voice or image to fool customers or staff. If you run a shop or organization, that is a good reason to establish simple verification habits with your team and your regulars, so a cloned 'owner' asking for an urgent payment or a changed bank detail gets double-checked rather than obeyed.

GOOD TO KNOW

If you must be public for business, keep family life on a separate private account, and set a verify-by-phone habit with your team for any money request that seems to come from you.

14. Checking Your App Permissions

What your apps can reach, and tightening it.

Beyond who can see your posts, it is worth a glance at what your apps themselves can reach on your phone — your microphone, camera, contacts, photos, and location. Over time, we grant these permissions without much thought, and some apps hold on to access they do not really need. Tightening these does not directly stop voice cloning, but it is good general hygiene and keeps apps from quietly gathering more of your voice, images, and connections than necessary.

Both iPhones and Android phones have a privacy or permissions section in Settings where you can see, app by app, what each one is allowed to use. Look especially at which apps can use your microphone and camera, and turn off any that have no good reason for it. If a simple game or a flashlight app has microphone access, for instance, that is worth switching off. The apps that genuinely need the microphone, like your phone or a video-call app, will keep it.

While you are there, review location access too, setting most apps to 'while using' rather than 'always,' and have a look at which apps can reach your contacts and photos. None of this is urgent, and you can do it slowly, but a periodic tidy-up of permissions keeps your phone sharing only what it should. As with the other settings, if the menus feel like a maze, it is a quick and painless job with a hand beside you.

TIP

A quick rule of thumb: if you cannot think of a reason an app needs your microphone, camera, or location, turn that permission off. The important apps will keep working fine.

15. A Word on Smart Speakers

The listening devices in your home.

Many homes now have smart speakers and voice assistants, and people sometimes worry these are quietly recording them for scammers. The honest picture is more mundane than the scary stories: mainstream assistants are designed to listen only for their wake word and to send audio to the company's servers mainly after that word, not to broadcast your living room to criminals. The real privacy questions are about the company's own data practices, which is a different topic from voice-cloning scams.

Still, if these devices concern you, you have sensible controls. Most let you review and delete your voice recordings, turn off the saving of recordings, and mute the microphone with a button when you want certainty. Using those controls is reasonable, and it is entirely your choice how much you want these devices in your home. For the specific worry of this guide — a scammer grabbing your voice — your public social-media videos are a far easier and more likely source than a smart speaker.

So keep the risks in proportion. By all means review and delete your assistant's recordings, mute it when you like, and set it up the way that feels comfortable. But do not let worry about the speaker on the counter distract you from the bigger, easier sources — public talking videos and voicemail greetings — or from the one habit that matters most, which remains verifying any suspicious call by reaching the person another way.

GOOD TO KNOW

Smart speakers mostly listen only for their wake word, and you can review, delete, and mute as you like. For voice-clone worries, your public videos are the easier target to address first.

16. Keeping Settings From Drifting

A quick re-check now and then.

One frustrating truth about privacy settings is that they can drift. App updates occasionally reset or change options, new features arrive turned on by default, and a setting you were sure you fixed can quietly revert. This is not usually malice; apps change constantly. But it means privacy is not a one-time job you finish and forget — it is more like checking the smoke detectors, a quick revisit every so often to make sure nothing has slipped.

A simple habit keeps you ahead of the drift: once or twice a year, perhaps when the clocks change, spend a few minutes running back through your main accounts' privacy settings to confirm they are still where you want them. Pay special attention right after a big app update, which is when defaults most often shift. It takes only a few minutes when you know what you are looking for, and it catches the quiet changes before they matter.

You do not need to track every update or become a settings expert. Just pair the re-check with something you already remember to do twice a year, and keep this guide or your checklist handy to walk through. And if a familiar menu suddenly looks different and you cannot find an option, that is a normal, common frustration and a perfectly good reason to call for a hand rather than giving up on it.

GOOD TO KNOW

Pin privacy to a date you already remember — like changing the clocks — and re-check your main accounts then. A twice-a-year glance keeps drifting settings from catching you out.

17. A Word on Face and Photos

Deepfake video needs images, too.

While this guide focuses on your voice, the same technology can use your face, so a quick word on images is worthwhile. Deepfake video tools learn from photos and video of a person, and public, high-quality pictures and clips of your face make that easier. The good news is that the same privacy settings you have just adjusted protect your face at the same time as your voice — tightening who can see your posts shrinks the pool of images too.

You do not need to become secretive about photos or stop sharing pictures of a lovely day. But a little thought helps: keeping your accounts friends-only, being cautious about posting lots of clear, forward-facing video of yourself publicly, and asking others not to tag or reshare your images publicly all reduce the raw material available. As with voice, the aim is to be a harder target, not to vanish from your own family's photo albums.

And as always, the settings are the lighter layer. If a 'video call' ever seems to show a familiar face asking for money or urgent action, the face on the screen is no longer proof, just as the voice on the phone is not. The same verify-another-way habit applies: confirm through a channel you trust before you act, no matter how real the person looks. Settings make you harder to fake; the habit makes the fake useless.

GOOD TO KNOW

Tightening your post privacy protects your face and your voice at once, since both are grabbed from the same public posts. One round of settings covers both.

18. What Settings Can't Do

An honest word about the limits.

I want to be straight with you about the limits, because overconfidence is its own danger. Tightening your privacy settings reduces how easily a stranger can grab your voice and face, but it cannot guarantee that no clip of you exists anywhere. Friends can reshare, old recordings may linger on others' pages, organizations post things you do not control, and app settings sometimes reset after updates. A locked-down account is a harder target, not an invisible one.

This matters because the danger is not really that a clip of your voice exists — some clip very likely does, for most of us. The danger is acting on a phone call or video just because it sounds or looks like someone you trust. No amount of privacy setting changes that, which is why I keep returning to the callback. Settings shrink the scammer's toolkit; they do not change the one rule that actually keeps you safe when a convincing fake reaches you anyway.

So do the settings, absolutely — they are worth it, and they help. But do not let tightening them lull you into trusting a voice or a face more than you should. Treat the settings as locking your windows and the callback habit as your deadbolt. Both together make a safe home; the deadbolt alone is far better than locked windows alone. Keep the deadbolt in mind above all.

WATCH OUT

Do not let a private account make you drop your guard on the phone. A scammer needs only one old clip from anywhere. The voice is still never proof — always verify by calling back.

19. The Callback Habit, One More Time

The protection that works even if a clip got out.

Because it is the true heart of your safety, let me state the callback habit plainly here, even though it has its own full guide. If you ever receive a call or message with an emergency and a request for money or secrecy — especially one that sounds like a loved one — you do not act on it. You say you will call right back, you hang up, and you reach that person on the number you already have saved for them. If you cannot reach them, you call another family member who can.

This works even if a scammer has a perfect clone of a voice, because it does not depend on the voice at all. They control the call that reached you; they do not control the number you dial out. When you call your loved one's real phone, you step entirely outside the scam. That is why the callback protects you even when every privacy setting in the world failed to keep some clip from getting out — and some clip usually does.

A family safe word is a fine backup for the rare times you cannot reach someone: a private word an outsider could not guess and you would never post online, which a real loved one knows and a clone does not. Settings, the callback, and a safe word together form a calm, layered protection. But if you keep only one thing in your heart, keep the callback — it is the one that holds when everything else slips.

TIP

I have separate guides on the callback test and on setting a family safe word. Ask me for them, or find them with the other safety guides on my website.

20. A Gentle Settings Checklist

Work through it at your own pace.

Here is a simple checklist to work through whenever you have a quiet few minutes. There is no need to do it all in one sitting; one item a day is perfectly fine. Each one you complete makes you a little harder to target, and you can feel good about every single one, however small it seems.

- Facebook: set future posts to Friends, and run 'Limit past posts.'
- Instagram: turn on 'Private account' and tidy your follower list.
- TikTok: turn on 'Private account' and turn off video downloads.
- YouTube: switch family and talking videos from Public to Unlisted or Private.

- Voicemail: switch to the phone's default greeting, or keep yours very short.
- Ask the grandkids to lock down their talking videos too.
- Remember the callback habit for any phone or video that asks for money or secrecy.

If any item on this list sends you digging through menus that do not look the way I described, do not get frustrated — apps change, and phones differ. Look for the underlying idea (who can see this, is it public or private, can it be downloaded), and if it still will not cooperate, set it aside and ask for a hand. This is exactly the kind of small, fiddly task that is quick and painless with someone sitting beside you.

TIP

Print this checklist or keep it by the computer, and tick off one item whenever you have a spare few minutes. Slow and steady gets the whole thing done without any stress.

21. Questions People Ask Me

The ones that come up again and again.

If I make everything private, will my family still see my posts? Yes. Private and friends-only settings keep your existing friends and approved followers; they only shut out strangers. The people you actually share with will still see everything, so you lose nothing that matters.

I've already posted public videos for years — is it too late? Not at all. Tools like Facebook's 'Limit past posts' and YouTube's per-video setting let you tighten old posts now. You cannot recall a clip someone already saved, but you can close the door going forward and shrink what is still out there.

Isn't it easier to just delete all my accounts? You can, but you do not need to, and you would lose the real joy of staying connected with family. Tightening settings keeps the good and removes most of the risk. Disappearing entirely is a big step that privacy settings make unnecessary for most people.

If my accounts are private, can I relax about strange phone calls? No — and this is the most important answer. A scammer needs only one old clip from anywhere, and some usually exists. So keep verifying by calling back no matter how locked-down your accounts are. Settings help, but the callback is what truly protects you.

22. A Five-Minute Family Privacy Setup

Do it together, and everyone benefits.

Privacy protects a family best when the whole family does it together, because a scammer can clone any member's voice to target any other. A short, shared session — perhaps at a holiday or a Sunday visit — lets everyone tighten up at once and turns it into a normal family habit rather than one person's lonely chore. Here is a simple plan you can run together in a few minutes.

- 1 Everyone sets their main social account to friends-only or private.
- 2 Everyone turns off video downloads where the app allows it (like TikTok).
- 3 Everyone switches to a plain or default voicemail greeting.
- 4 The younger members help the older ones, and the older ones share why it matters.
- 5 Everyone agrees on the callback habit, and the family picks a private safe word.

GOOD TO KNOW

Doing this as a family removes any sense that one person 'needs watching.' It is simply how your family handles its privacy — and it protects everyone in every direction.

23. 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://www.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](https://www.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](https://www.ohioattorneygeneral.gov).
- If your identity may be exposed, visit [IdentityTheft.gov](https://www.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.

24. When to Just Call Me

A calm second opinion costs you nothing.

If something about your privacy settings and what of your voice and face is public 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.

25. 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.

You do not have to disappear to be safe — you only have to close a few easy doors. Take it one setting at a time, ask for help when a menu is fiddly, and share your life with the people you love. If you'd like a hand tightening your accounts, I am a phone call away and glad to sit down with you.

CHEAT SHEET

Everyday Cheat Sheet

The big idea

Close the easy doors so strangers can't grab your voice and face — but remember the callback is your real protection.

App by app

- Facebook: future posts to Friends; run 'Limit past posts.'
- Instagram: turn on Private account.
- TikTok: Private account, and turn off downloads.
- YouTube: family videos to Unlisted or Private.
- Voicemail: use the phone's default greeting.

And always

- 1 Ask the grandkids to lock down their videos too.
- 2 Ask friends not to reshare your clips publicly.
- 3 A voice is never proof — call back to verify.
- 4 Set a family safe word as a backup.
- 5 Need help with a menu? Call Bill.

WATCH OUT

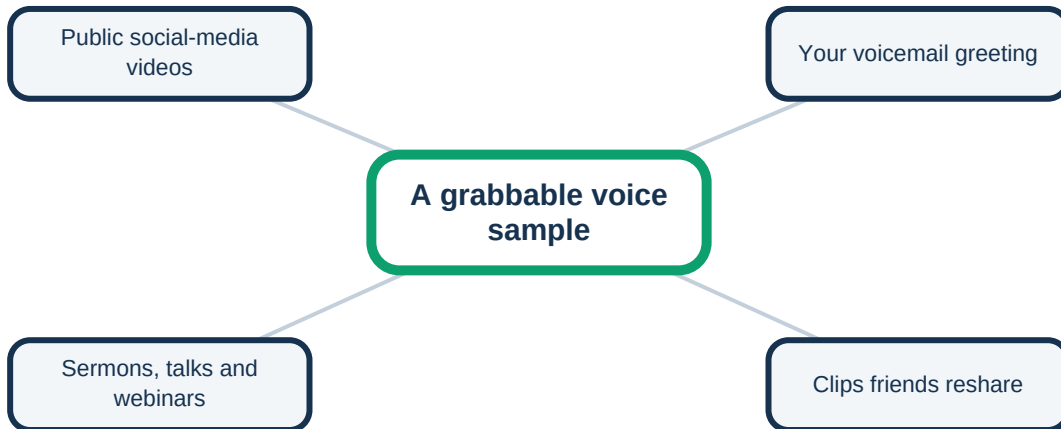
A private account is a harder target, not an invisible one. A friend can reshare and old clips linger — so never let locked-down settings tempt you to trust a voice on the phone.

AT A GLANCE

A Picture to Follow Along

Where Your Voice Sits in Public

The everyday sources worth tightening.



Close the easy doors - set talking videos to friends-only.

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

AT A GLANCE

A Second Look

Lock It Down, Step by Step

A few minutes of settings makes you a harder target.

- 1 Set social accounts to friends-only or private
- 2 Turn off video downloads where you can
- 3 Switch to a plain or default voicemail greeting
- 4 Make old public videos private or unlisted
- 5 Ask the grandkids to lock their videos too
- 6 Still trust the callback - the voice is never proof

Settings are the windows; the callback habit is the deadbolt.

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.