



Deepfake Video Calls — When Seeing Their Face Isn't Proof

Live deepfake video calls are here — and the simple check that still protects you.

————— **An Extended Guide · No. 1632 · 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. What a Deepfake Video Call Is	5
3. The Case That Made Headlines	6
4. Where You Might Meet One	6
5. The One Habit That Protects You	7
6. A Business Rule That Stops the Big Losses	8
7. The Romance-Scam Version	9
8. Spotting a Deepfake — With Low Expectations	10
9. Why Your Eyes Betray You Here	10
10. A Family Safe Word Works Here Too	11
11. Protecting Your Own Image	12
12. The Group-Call Trick	13
13. How the Setup Usually Starts	14
14. A Word on Avatars and Filters	14
15. Teaching Your Team or Family	15
16. If You're Not in Business	16
17. If You've Been Targeted	17
18. Keeping Everyday Calls Joyful	17
19. Questions People Ask Me	18
20. A Five-Minute Setup	19

21. Reporting It — and Why It Helps 19

22. When to Just Call Me 20

23. Contact Card & a Warm Close 21

Everyday Cheat Sheet 21

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

A video call used to feel like proof — if you could see their face, surely it was really them. That is no longer safe. Technology can now fake a familiar face and voice on a live video call. So if a video call brings an urgent request for money, secrecy, or sensitive information, you don't act on it just because the face looks right. You pause and confirm through another channel you already trust — a callback on a known number, a question only the real person could answer, or a family safe word.

- 1 A video call brings an urgent request — money, a transfer, secrecy, a password.
- 2 The face and voice look and sound like someone you trust.
- 3 Remember: a live face can now be faked, so seeing isn't proof.
- 4 Pause; don't act on the call alone.
- 5 Verify another way — call back on a known number, or ask something only they'd know.

WATCH OUT

Deepfake video is mostly used against businesses and urgent money requests, not casual family chats. Your everyday video calls with the grandkids are almost certainly fine — it's the urgent money-and-secrecy ones to double-check.

1. Why I Wrote This One

Seeing is no longer believing — but you're still safe.

In more than thirty years of helping people around Portage County with their technology, I have watched 'proof' get steadily less reliable. First we learned that a voice on the phone could be faked. Now I need to tell you that a face on a video call can be faked too, live, in real time. It sounds like science fiction, and I understand if it is unsettling. But I would rather you hear it from me, calmly and with a clear plan, than be caught off guard.

Let me put the fear in proportion right away, because proportion matters. This technology is real, but today it is mostly aimed at businesses and large, urgent money transfers, not at casual family video chats. Your regular video calls with the grandkids are almost certainly exactly who they appear to be. The danger lies in a specific situation: a video call that brings an urgent demand for money, secrecy, or sensitive information. That is the narrow case this guide is about.

And as always, there is a simple habit that keeps you safe, even when your own eyes and ears are fooled. You do not have to become an expert at spotting fakes — that is a losing

game as the technology improves. You only have to apply one rule to urgent requests: verify on another channel before you act. We will walk through how deepfake video calls work, a real case that made headlines, where you might encounter one, and exactly how to protect yourself and your business. No fear, no jargon, no rush.

WATCH OUT

If you run a business, handle money for a church or club, or help family with finances, this is the guide to share. The urgent 'boss on a video call' transfer is where this scam does its worst damage.

2. What a Deepfake Video Call Is

The plain-English version.

A deepfake is video, audio, or imagery that a computer has generated or altered to show a real person saying or doing something they never did. For a long time, deepfakes were pre-recorded — a fake video posted online. What is newer, and what this guide is about, is that the technology can now do this live, during a real-time video call, so the person you appear to be talking to on screen is a computer-generated fake of someone real.

In practice, a scammer can take video and audio of a target — a company executive, a public figure, sometimes an ordinary person with enough footage online — and use software to generate a convincing live impersonation. On the call, the fake face moves, speaks, and responds, mimicking the real person well enough to fool colleagues who know them. The effect is powerful precisely because we have all spent our lives treating 'I can see and hear them' as solid proof of identity.

It is important to know both what this can and cannot do, to keep the fear realistic. The technology is impressive but demanding, which is why it is currently aimed at high-value targets rather than sprayed at everyone like robocalls. And like a voice clone, a deepfake of a person copies their appearance and manner, not their private knowledge or their genuine connection to you. Those limits are exactly what your verification habit will exploit, no matter how good the fake on screen becomes.

GOOD TO KNOW

A deepfake copies how someone looks and sounds, not what they privately know or their real phone number. That gap is what a second-channel check exploits, even against a flawless fake.

3. The Case That Made Headlines

A real company, a real multi-million-dollar loss.

This is not a hypothetical worry, and one widely reported case shows exactly how serious it can be. A finance employee at a large international engineering firm was tricked into transferring the equivalent of roughly twenty-five million dollars after joining what seemed to be a routine video conference. On that call were people who appeared to be the company's chief financial officer and several colleagues the employee recognized.

Every one of those people on the video call was a deepfake — convincing fake video and voice of real coworkers. The employee had initially been suspicious of an unusual request that arrived by message, but the video call put those doubts to rest, because the faces and voices looked and sounded exactly like people he knew and worked with. Reassured by seeing his 'colleagues,' he followed the instructions and authorized a series of transfers before the fraud was discovered.

The lesson in that story is the whole of this guide in miniature: seeing and hearing familiar people on a screen is no longer proof that they are really there. If a careful professional at a major firm can be fooled by a live fake of people he knew, then none of us should feel foolish for being fooled, and all of us should adopt the habit that would have stopped it — verifying an urgent money request through a separate, trusted channel before acting, no matter how real the video looks.

GOOD TO KNOW

In that case, the worker's doubts were erased by the video call itself. That is the trap: the fake meeting is used precisely to override the suspicion that would otherwise save you.

4. Where You Might Meet One

The situations that carry real risk.

Because this technology is demanding, it is aimed at situations where the payoff is large or the target is specific. Knowing where the real risk lies lets you relax about everyday calls and stay alert in the few settings that matter. Here are the situations where a deepfake video call is a genuine concern.

- A business video call where a 'boss' or executive urgently directs a wire transfer, a payment, or a change to bank details.
 - A finance or bookkeeping role being asked, on video, to move money or share company credentials.
 - A 'colleague' or 'vendor' on video pressing for an urgent, unusual financial action.
 - A romance or long-con scam where a 'partner' finally agrees to a video call to prove they're real — then asks for money.
 - An investment or crypto pitch featuring a live 'advisor' or a familiar face urging you to act.
- Notice the common thread: every one involves money and urgency, and most involve a position of authority or trust being borrowed. By contrast, your spontaneous video chat with a grandchild about their day carries essentially no deepfake risk — there is nothing in it for a scammer, and no urgent money request. So you do not need to view every video call with suspicion. You need to apply extra care specifically when a video call turns to urgent money, secrecy, or sensitive information.

TIP

Let the combination 'video call + urgent money or secrets' be your trigger for extra care. Ordinary video calls with no money request are almost always exactly who they seem.

5. The One Habit That Protects You

Verify urgent requests on another channel.

Here is the whole defense: for any urgent request involving money, secrecy, or sensitive information that comes over a video call, you do not act on it from the call alone — you confirm it through a separate channel you already trust before you do anything. That might mean hanging up and calling the person back on their known number, reaching them through a different method you have used before, or asking something only the real person would know.

This works because it does not depend on your ability to spot a deepfake, which is a game you will increasingly lose as the technology improves. The scammers pour their effort into making the face and voice on the call convincing. They cannot control the separate channel you use to check — the real person's actual phone, a known email thread, an in-person confirmation. When you reach the real person another way, the deepfake on the call becomes irrelevant, because you are no longer relying on it.

The key is that the verification must be genuinely separate from the suspicious call. Do not verify by asking the person on the video call to confirm they are real — of course the fake will say yes. Do not use a number or link they provide on the call. Step entirely outside that conversation: call the known number, start a fresh message to the address you already have, or simply walk down the hall and ask in person. Separate channel, every time.

WATCH OUT

Never verify a suspicious call by asking that same call to prove itself — the fake will happily confirm. Step outside it: a known number, a fresh message, or a walk down the hall.

6. A Business Rule That Stops the Big Losses

For anyone who moves money at work.

Since deepfake video is aimed squarely at business money transfers, the single most valuable protection for any organization — a company, a shop, a church, a nonprofit, a club — is a simple, ironclad rule: no money moves and no payment details change on the strength of a video call, a message, or an email alone. Any such request is confirmed through a separate, known channel before anyone acts, no exceptions, including when it appears to come from the boss.

Make it concrete and routine so it carries no awkwardness. Decide in advance that a wire, a large payment, or a change to a vendor's bank details always requires a confirmation call to a known number, or an in-person okay, regardless of how the request arrived or who seems to be making it. When this is simply the standing policy that everyone follows, no employee has to feel they are questioning the boss — they are following the rule that protects the boss and the business alike.

This one habit would have stopped the headline case and stops nearly every version of the scam, because the deepfake call cannot survive an independent confirmation to the real executive's real phone. If you own or help run a small organization, setting up this verification step is the highest-value thing you can do against this threat, and it costs nothing but a moment's pause. It is exactly the kind of sensible safeguard I am glad to help a local business put in place.

WATCH OUT

'The CEO on video told me to wire it urgently' is the exact setup of the biggest losses. A standing rule — confirm every transfer on a known channel — stops it cold.

7. The Romance-Scam Version

When a video call is used to 'prove' a lie.

There is a personal version of this worth understanding, because it undoes a piece of advice people have relied on. For a long time, the standard guidance for online romance scams was 'insist on a video call — a scammer won't do one.' That was good advice once. Now, deepfake technology means a scammer can appear on a video call with a convincing face, which can falsely reassure a victim that their online sweetheart is real before the requests for money begin.

So a successful video call can no longer be treated as proof that an online relationship is genuine. The deepfake may be brief, glitchy, or 'shy' about the camera, with excuses for poor quality, or it may be startlingly convincing. Either way, the video call does not override the real protection against romance and investment scams, which is not about proving the person is real at all. It is about keeping money completely separate from any relationship that began online.

That is the rule to hold: you never send money, invest, or share financial access because of someone you met online, no matter how real they seem on a video call. The face on the screen is not the thing that decides it; the fact that the request came from an online relationship is. If you have read my guides on romance scams and pig-butchering, this is the same money boundary, now reinforced against a video call that can no longer be trusted as proof.

WATCH OUT

'We video-chatted, so they must be real' is no longer safe. A deepfake can pass a video call. Keep money entirely out of any online relationship, whatever the screen shows.

8. Spotting a Deepfake — With Low Expectations

Clues that sometimes help, and why not to rely on them.

People always ask how to tell if a video call is a deepfake, and I will share the clues — but with an honest warning first. Today's fakes can be caught sometimes by these signs, but the technology improves constantly, and a good fake may show none of them. So treat these as a bonus that might confirm your suspicion, never as a reliable test. The absence of flaws proves nothing, which is why the verification habit remains your real protection.

- Unnatural blinking, or eyes and gaze that seem slightly off.
- Facial movements, lip-sync, or expressions that don't quite match the words or feel subtly wrong.
- Odd lighting, blurring, or shimmering around the edges of the face, hair, or glasses.
- A reluctance to do something simple and live on request — turn their head, wave a hand in front of their face, or hold up a specific object.
- Audio and video slightly out of sync, or a voice that sounds a touch flat or processed.

One mildly useful live test: ask the person to do something unexpected and physical on camera — slowly turn their head to the side, pass a hand in front of their face, or hold up a particular object and describe it. Some current deepfakes struggle with these. But a capable fake may handle them fine, so even this is not proof. If you are at the point of running tests, you are already suspicious enough that the right move is simply to stop and verify through a separate channel, which settles it with certainty.

GOOD TO KNOW

If you're suspicious enough to be testing a video call for fakery, just stop and verify on another channel. That gives certainty; squinting for glitches does not.

9. Why Your Eyes Betray You Here

The deep trust that makes this work.

It is worth understanding why this scam is so effective, because understanding it keeps you humble and safe. We are wired, from birth, to trust faces. Seeing and hearing a familiar person is one of the most fundamental forms of recognition we have, far deeper and more automatic than reading words or hearing a voice alone. A video call activates that deep trust completely, which is exactly why 'I saw their face' has always felt like the end of any doubt.

That deep, automatic trust is precisely what the deepfake hijacks. When the finance worker in the headline case saw his colleagues' faces, his suspicion simply dissolved, not through any failure of intelligence but because his brain did what every human brain does — treated seeing familiar faces as proof. The scam is engineered to trigger that response and ride it straight past our caution. None of us is immune, because the response is not a flaw we can train away.

Recognizing this does two useful things. It removes shame: being reassured by a familiar face is human nature, not gullibility. And it motivates the one change that works: consciously demoting 'I can see them' from proof to mere appearance, at least for urgent money requests. You cannot stop your eyes from trusting a face, but you can decide, in advance, that for anything involving money or secrets, a face on a screen is not enough — and that a separate confirmation is required. That decision, made calmly ahead of time, is what holds when your eyes say otherwise.

GOOD TO KNOW

Trusting a familiar face is hardwired, not a weakness. You can't switch it off — but you can decide in advance that, for money, a face on a screen isn't proof.

10. A Family Safe Word Works Here Too

The backup that beats a faked face.

The family safe word you may have set up against voice-cloning phone scams works beautifully against deepfake video calls as well, and it is worth keeping in mind for personal situations. If a video call seems to show a loved one in urgent trouble asking for money, you can ask for the family safe word — the private word or phrase your family agreed on in advance that an outsider could not know. A real loved one knows it; a deepfake does not, because knowing is not the same as appearing.

This is powerful because it tests knowledge, which the deepfake lacks, rather than appearance, which it fakes. The fake can reproduce the face and voice flawlessly and still be stopped cold by a simple question it cannot answer. Combined with the separate-channel callback, the safe word gives you two sturdy tools that do not depend at all on whether the image on your screen is real, which is exactly the kind of protection you want as fakes keep improving.

If your family has not set up a safe word yet, it is a five-minute conversation well worth having, and it now guards against both faked voices on calls and faked faces on video. Pick something private and odd, never posted online, agree on it together, and teach the rule: if someone contacts you in a panic about money and cannot give the word, slow down and verify before acting. I have a separate guide just on choosing and using a family safe word if you would like the details.

TIP

A family safe word tests knowledge, which a deepfake lacks. Ask for it on any urgent 'loved one in trouble' video call — the real person knows it; the fake can't.

11. Protecting Your Own Image

Reducing the raw material for a fake of you.

Just as a voice clone needs a sample of your voice, a deepfake of you needs images and video of your face. You cannot erase your image from the world, and you should not have to hide, but a few sensible habits reduce how much clear, usable footage of you sits publicly available, which makes you a slightly harder target — particularly worthwhile if you are a business owner, a public figure in your community, or simply want to be prudent.

The same privacy settings that protect your voice protect your face, because both are grabbed from the same public posts. Setting your social-media accounts to friends-only rather than public, being a little thoughtful about posting lots of clear, forward-facing video of yourself to fully public accounts, and asking others not to reshare your images publicly all shrink the pool of raw material. None of this requires leaving social media or giving up sharing with the people you love; it is just closing the easy doors.

Keep it in proportion, though. For most people, the realistic risk is not that someone will deepfake you, but that someone will deepfake a known executive or a public figure, or will use a faked face against you in an urgent money request. So tightening your image privacy is a reasonable bonus layer, while the verification habit remains the main event. Business owners and people with a public profile have the most reason to be careful here; everyone else can simply keep sensible privacy and lean on the habit.

TIP

Tightening your post privacy protects your face and your voice at once, since both come from the same public posts. It's a worthwhile bonus — but the verification habit is the real shield.

12. The Group-Call Trick

Several fake 'colleagues' on one call.

One especially convincing twist, seen in the headline case, is faking not just one person but several on the same call. When a video meeting appears to include your boss, a couple of familiar colleagues, and perhaps an outside advisor, all nodding along and reinforcing the request, the pressure to comply is enormous. Surely, you think, they could not all be fake. That instinct — safety in numbers — is exactly what the trick exploits.

But if the technology can fake one convincing face and voice, it can fake several on the same call, especially in a scripted meeting where the 'participants' mostly agree and press in the same direction. A room full of familiar faces endorsing an urgent transfer is not independent confirmation; it is one scam wearing several masks. The apparent consensus is manufactured, every bit as fake as a single impersonation would be, and no more trustworthy for the extra faces.

So do not let a crowd of familiar faces substitute for real verification. The rule does not change because several 'people' agree: any urgent money request still gets confirmed through a separate, known channel before you act. In fact, a surprise meeting where multiple authority figures all push the same unusual, urgent financial action, and discourage you from stepping away to check, should raise your caution rather than lower it. Real colleagues do not mind you confirming; a coordinated fake needs you not to.

WATCH OUT

Several familiar faces on a call agreeing isn't independent proof — if one can be faked, so can several. A crowd pushing an urgent transfer is a reason to step away and verify, not to comply.

13. How the Setup Usually Starts

The video call rarely comes out of nowhere.

A deepfake video call is usually the middle of a scam, not the beginning, and knowing the setup helps you catch it earlier. It often starts with a message — an email or chat from a 'boss,' a 'colleague,' or a 'vendor' raising an urgent matter: a confidential deal, a pressing payment, a problem that needs quick, quiet handling. The message primes you to expect the call and to treat it as legitimate before the fake face ever appears.

Then comes the invitation to a video meeting 'to discuss it,' which is the master stroke. If the initial message alone raised any doubt — and in the headline case it did — the video call is deployed precisely to crush that doubt, because seeing the familiar faces feels like ironclad proof. The scammers understand that a suspicious employee who would question an email will often comply after 'seeing' the boss, so the call exists to override exactly the caution that would otherwise save you.

This sequence gives you an early warning. When an unusual, urgent, confidential money request arrives by message and is quickly escalated to a video call that conveniently resolves your doubts, treat that very pattern as suspicious rather than reassuring. The more a surprise request leans on urgency and secrecy and then uses a video call to dissolve your questions, the more it deserves an independent check. The call being offered 'to reassure you' is itself a reason to verify elsewhere.

WATCH OUT

A video call offered to 'put your mind at ease' about an urgent, secret money request is doing a job: dissolving your doubt. Let that pattern raise your caution, not lower it.

14. A Word on Avatars and Filters

Keeping the technology in perspective.

You may have seen playful face filters and cartoon avatars on video calls and social media — features that put bunny ears on you or turn you into a talking animal. It is natural to wonder whether these are the same thing as a deepfake, and understanding the difference keeps your worry proportioned. Those everyday filters are obvious, consensual fun; a malicious deepfake is a deliberate, convincing impersonation of a specific real person without their consent, aimed at deception.

The technology does sit on a spectrum, and the harmless, obvious end is far more common in daily life than the dangerous end. The vast majority of what you encounter — the grandchild's silly filter, the app that makes everyone look like a potato — is plainly not real and fools no one. The malicious deepfake is a specialized tool wielded by criminals against specific, high-value targets, which is why it remains rare in ordinary settings even as it makes alarming headlines.

Keeping this perspective matters so you neither panic at every video effect nor dismiss the real threat. You do not need to fear your grandchild's funny filters, and you do not need to scrutinize every call for signs of fakery. You simply apply the one habit — verify urgent money requests on a separate channel — in the narrow situations that warrant it, and otherwise enjoy video technology, filters and all, for the fun and connection it brings.

GOOD TO KNOW

Silly face filters are obvious, consensual fun and fool no one. A malicious deepfake is a deliberate impersonation of a real person — rare, targeted, and the only kind worth guarding against.

15. Teaching Your Team or Family

Everyone who could get the call should know.

Protection against this scam works best when everyone who might receive such a call understands it in advance — not just the owner or the oldest family member, but anyone who handles money or could be impersonated. A scammer only needs to find the one person who has not heard of deepfake video calls and who will act on an urgent 'boss' request without verifying. Closing that gap means making sure the whole team or family shares the knowledge and the rule.

For a business, church, or club, this is a short, practical conversation: explain that faces on video calls can now be faked, share the standing rule that no transfer or payment-detail change happens on a call, message, or email alone, and make clear that following the rule is expected and welcome, never an insult to anyone's authority. Reassure staff, especially junior ones, that they will never be in trouble for pausing to confirm an urgent money request — that pausing is exactly what the organization wants.

For a family, fold it into the same conversation where you set your safe word and callback habit. Make sure anyone who helps with family finances, and anyone whose face or voice

could be copied, understands that an urgent money request on a video call gets verified another way. The goal in both settings is the same: no single uninformed person left as the weak point, and a shared, blame-free habit that everyone follows together.

WATCH OUT

Tell your team, in writing: 'You will never be in trouble for pausing to confirm an urgent money request.' Removing the fear of questioning the boss is what makes the rule actually work.

16. If You're Not in Business

The personal version still matters.

If you do not run a business or handle money at work, you might wonder whether this threat really touches you. It does, in a few personal ways worth knowing, even though the biggest dollar losses are on the business side. The personal versions lean on the same faked-face trust, aimed at your heart or your savings rather than a company's wire transfers.

The main personal risks are the romance-scam version, where a deepfake video call is used to 'prove' an online sweetheart is real before asking for money, and the loved-one-in-trouble version, where a faked face could reinforce an urgent plea for help. There is also the investment angle, where a live 'advisor' or a familiar celebrity face urges you into a scheme. In each, the faked face is used to lend false credibility to a request that your money rules should already stop.

So the personal defenses are ones you likely already know from my other guides: never move money because of someone you met online, no matter how real they seem on video; verify any 'loved one in trouble' request through a callback or a safe word; and never invest based on a video or an unsolicited contact. The deepfake video call does not introduce a new rule for your personal life — it simply reinforces how important those existing money boundaries have become, now that a video call can no longer serve as proof.

GOOD TO KNOW

For personal life, the deepfake video call adds no new rule — it just means 'we video-chatted, so it's real' no longer holds. Your existing money boundaries still protect you.

17. If You've Been Targeted

Steps whether or not money moved.

If you suspect you have been on a deepfake video call, or worse, acted on one, here is what to do. First, the good news about catching it: if you grew suspicious and did not send money or share sensitive information, you have avoided the harm — simply disengage, do not act on anything from the call, and verify the real person's situation through a known channel. Then warn whoever else might be targeted, since these scams often probe several people in an organization or family.

If money did move or you shared sensitive access, act quickly and calmly. For a business, that means contacting your bank immediately to try to stop or recall the transfer, since speed can occasionally help; alerting your organization's leadership and anyone who handles finances; and changing any credentials that were exposed. For a personal loss, call your bank or card company right away, change affected passwords, and treat any shared personal information as exposed, using [IdentityTheft.gov](https://www.identitytheft.gov) if needed.

- 1 Stop acting on the call immediately; don't send more money or share more access.
- 2 Contact your bank right away to try to stop or recall any transfer — minutes matter.
- 3 Verify the real person's or executive's situation through a known, separate channel.
- 4 Change any exposed passwords and credentials; turn on a second lock.
- 5 Warn others who might be targeted, document everything, and report it (FBI [ic3.gov](https://www.ic3.gov), FTC).

GOOD TO KNOW

For business wire fraud especially, report to the FBI at [ic3.gov](https://www.ic3.gov) as fast as possible — rapid reporting occasionally helps recover or freeze transferred funds.

18. Keeping Everyday Calls Joyful

Don't let this spoil connection.

I want to end the teaching part with reassurance, because it would be easy to come away afraid to video-call your own family, and that would be a real loss. Video calls are a wonderful gift, letting grandparents see grandchildren grow, keeping far-flung families close, and bringing faces into our homes across any distance. I do not want this guide to take an ounce of that joy from you. The overwhelming majority of your video calls are exactly who they appear to be.

Keep the risk in its proper, narrow place. Deepfake video calls are a real but targeted threat, aimed mainly at business money transfers and at urgent money requests dressed up as a trusted face. A spontaneous call to say hello, show off a new haircut, or read a bedtime story has nothing in it for a scammer and carries essentially no risk. You can and should enjoy those freely, without a shadow of suspicion.

The habit is simply a seatbelt for the rare dangerous moment, not a reason to stop driving. You click it only when the conditions call for it — a video call that turns to urgent money, secrecy, or sensitive information — and otherwise you video-chat with an open heart. Because you know you will pause and verify in that one narrow situation, you can relax everywhere else. The plan buys back your peace of mind rather than stealing it.

GOOD TO KNOW

Your everyday video chats are almost certainly real and safe. The habit is a seatbelt for the one risky situation — urgent money on a video call — so you can relax about all the happy ones.

19. Questions People Ask Me

The ones that come up again and again.

Should I be worried about my regular video calls with family? Almost certainly not. Deepfake video is demanding and aimed at high-value, urgent money situations, not casual chats. Enjoy your family calls. Just apply extra care if any video call turns to an urgent request for money, secrecy, or sensitive information.

Can't I just look closely and spot the fake? Sometimes, today — but the technology improves constantly and a good fake may show no flaws. Spotting fakes is a game you'll increasingly lose. The reliable protection is to verify urgent requests on a separate channel, which works no matter how good the fake is.

The person on the call insisted they were real and got annoyed when I hesitated — doesn't that mean they're genuine? No. A fake will happily insist it's real, and pressure or irritation when you want to verify is actually a warning sign. A genuine person, especially a real boss or loved one, will understand you confirming an urgent money request through another channel.

I run a small business — am I really a target? Any organization that moves money can be targeted, not just big corporations. The fix is cheap and powerful: a standing rule that no

transfer or payment-detail change happens on a call, message, or email alone, always confirmed on a known channel. That one habit protects you.

20. A Five-Minute Setup

For your family and your business.

A little preparation makes this threat easy to handle. Do these once, at home and at work, and you will be well protected without having to think about deepfakes every time your phone rings. Match the steps to your situation — the family ones for everyone, the business ones if you move money for an organization.

- 1 Adopt the rule: urgent money, secrecy, or sensitive requests on a video call are always verified on a separate, known channel first.
- 2 Set a family safe word (private, odd, never posted) and teach the rule to everyone.
- 3 At work, make it policy: no transfer or payment-detail change on a call, message, or email alone — always confirm on a known number.
- 4 Save key people's real numbers so a verification callback is quick.
- 5 Tighten your social-media privacy to friends-only, which protects your face and voice together.
- 6 Pick one trusted person (and, at work, a clear confirmation contact) to check with when something feels off.

GOOD TO KNOW

The single most valuable step for an organization is the standing transfer-verification rule. It would have stopped the biggest reported loss, and it costs nothing but a moment's pause.

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, 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 a video call where the face on screen asks for money or urgent action 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.

Seeing a face on a screen is no longer proof of who you're talking to — but a quick check on a channel you trust always is. Slow down, verify, and call me anytime a video call doesn't sit right. I am only a phone call away, and glad to help.

CHEAT SHEET

Everyday Cheat Sheet

The one rule

A face on a video call is no longer proof. For any urgent request involving money, secrecy, or sensitive info, verify on a separate, known channel before acting.

When to be careful

- A 'boss' on video urging an urgent wire or payment.
- A request to change a vendor's bank details.
- An online 'sweetheart' who video-calls, then asks for money.
- Several familiar faces pushing one urgent transfer.
- Any video call that turns to money, secrecy, or passwords.

How to verify

- 1 Don't act on the call alone.
- 2 Call the person back on a known number.
- 3 Or ask a family safe word only they'd know.
- 4 At work: confirm every transfer on a known channel.
- 5 Never verify by asking the same call to prove itself.

GOOD TO KNOW

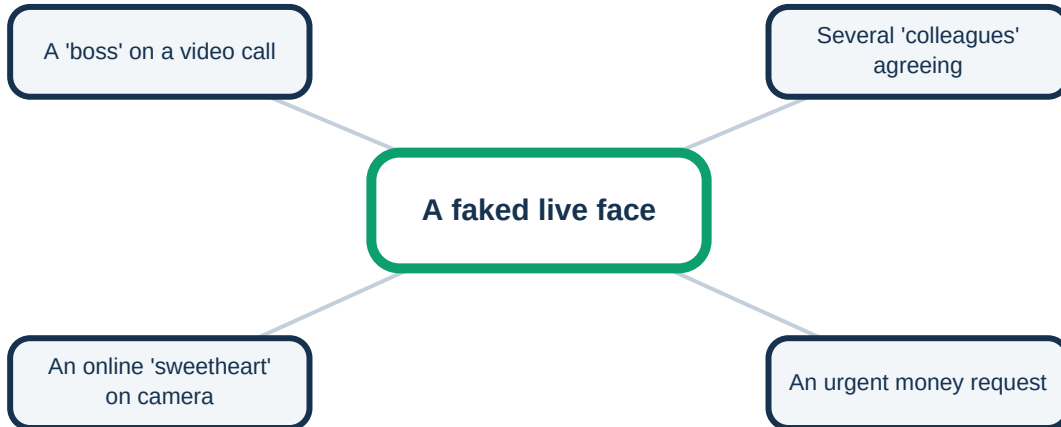
Everyday family video chats are almost certainly fine. The care is for the narrow case: a video call that turns to urgent money or secrets.

AT A GLANCE

A Picture to Follow Along

Why Seeing Isn't Proof Anymore

A familiar face on a live call can now be faked.



Your eyes trust a familiar face - so decide money needs more.

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

AT A GLANCE

A Second Look

The Check That Still Works

Confirm urgent requests on a channel you trust.

- 1 A video call brings an urgent money request
- 2 Remember: a live face can be faked now
- 3 Don't act on the call alone
- 4 Step outside it - call a known number
- 5 Or ask a family safe word only they'd know
- 6 Act only once you've confirmed a separate way

Never verify a suspicious call by asking that same call to prove itself.

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.