



Deepfake Extortion — "We Put Your Face in a Video"

A calm, steady guide to the fake-image threat — why it has no real power over you.

————— An Extended Guide · No. 1639 · 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. A Steady Word First 4
- 2. What Deepfake Extortion Is 5
- 3. The Golden Rule — Don't Pay 6
- 4. Don't Engage, Don't Panic 7
- 5. Why the Fake Has No Real Power 8
- 6. Where the Images Come From 9
- 7. It Is Not Your Fault 9
- 8. What to Do, Step by Step 10
- 9. Reporting and Getting Help 11
- 10. The Romance-Scam Doorway 12
- 11. Protecting Your Photos in Advance 13
- 12. If It's Targeting a Young Person 14
- 13. The Bluff-to-a-List Version 15
- 14. The Emotional Toll Is Real 16
- 15. Helping Someone Being Targeted 17
- 16. Questions People Ask Me 18
- 17. A Note on Prevention 18
- 18. You Will Get Through This 19
- 19. Reporting It — and Why It Helps 20
- 20. When to Just Call Me 21

21. Contact Card & a Warm Close 21

Everyday Cheat Sheet 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

If someone threatens to release an embarrassing or explicit image or video of you unless you pay, it is extortion, and the image is very often fake or AI-generated. The rules are clear and steady: do not pay, do not respond, do not panic. Paying does not make it stop — it marks you as a payer and invites more demands. Stop communicating, save the evidence, and report it to the authorities. This is a crime committed against you, not something you've done wrong, and help is available.

- 1 A threat demands money to keep a compromising image or video private.
- 2 Do not pay — paying only brings more demands, never safety.
- 3 Do not reply or engage further.
- 4 Save the evidence: the messages, the account, what was threatened.
- 5 Report it to the authorities (FBI at ic3.gov), and tell someone you trust.

GOOD TO KNOW

This is a sensitive and frightening topic. If it is happening to you, please know: it is not your fault, you are not alone, and there are people and resources ready to help you through it.

1. A Steady Word First

If this is happening, breathe — you're not alone.

If you are reading this because someone is threatening you — claiming to have an embarrassing or explicit image or video of you and demanding money to keep it quiet — I want you to take a slow breath before anything else. I know the fear and shame can feel overwhelming, that your heart is pounding and your mind is racing. You are going to be all right. This is a known, common crime, there is a clear and steady set of things to do, and none of this is your fault.

In more than thirty years of helping folks across Portage County with their technology, I have learned that the cruelest scams work by isolating a frightened person and rushing them. This one is built almost entirely out of fear and shame, and it has a weakness: the moment you understand how it works and that it has no real power over you, the fear begins to drain away. That understanding is what I want to give you here, calmly and without judgment.

So this guide will explain what deepfake extortion is, why the threat is usually hollow, and exactly what to do, step by careful step. It is written to steady you, not to alarm you. Whether this is happening to you right now, to someone you love, or you simply want to be prepared, you will come away knowing that this threat can be faced and defeated, and that you do not have to face it alone. Help is available, and we will get to how to reach it.

GOOD TO KNOW

If this is happening right now and you feel you cannot cope, please reach out to someone you trust immediately, and know there are crisis resources and authorities ready to help you this moment.

2. What Deepfake Extortion Is

The plain, calm explanation.

Deepfake extortion is a threat to release a compromising image or video of you — one that is usually fake, created or altered by a computer — unless you pay. 'Extortion' simply means demanding money or something of value through threats. The newer, 'deepfake' twist is that artificial intelligence can now take ordinary photos of a person, often pulled from social media, and alter them into fake explicit or embarrassing images that look real, which the criminal then threatens to send to your family, friends, or the world.

There are a few versions. In one, the criminal has genuinely fabricated a fake image using AI and your public photos. In another, very common version, the criminal has nothing at all — no real or fake image — and is simply bluffing, counting on your fear to make you pay before you think. In a third, which has sometimes involved real material obtained through manipulation, the dynamic is similar. In the great majority of mass extortion attempts, there is either a fake image or no image whatsoever.

The crucial thing to understand is that in all these versions, the criminal's only real weapon is your fear and shame. They cannot actually force you to do anything; they can only threaten and hope you panic. A fake image is just that — fake — and a bluff is nothing at all. Once you see that the entire scheme rests on frightening you into paying, you can begin to meet it with the calm, steady response that takes away its power. The threat is loud; its actual power over you is small.

GOOD TO KNOW

In most mass extortion attempts there's either a fake, AI-made image or no image at all. The criminal's only real weapon is your fear — not anything they actually hold over you.

3. The Golden Rule — Don't Pay

Why paying never makes it stop.

The single most important rule in extortion is this: do not pay. It feels counterintuitive when you are frightened and just want the threat to go away, but paying is the worst thing you can do, and understanding why is deeply steadying. Paying does not buy you safety or silence. It does the opposite: it confirms to the criminal that you are frightened, that you can be manipulated, and that you have money — which marks you as a valuable target and invites more demands, not fewer.

Extortionists who are paid almost always come back for more. The first demand becomes the first of many, each one justified by a new claim or a new deadline, because you have shown them that threats work on you. There is no version where you pay once and they honor a promise to disappear; that is simply not how these criminals operate. The money you send does not resolve the situation — it funds and encourages the people tormenting you, and it tells them to keep going.

So hold the golden rule firmly, even through the fear: you do not pay, no matter how convincing or frightening the threat. This is the advice of law enforcement and victim-support experts universally, and it is the thing that most reliably brings these situations to an end, because an extortionist who gets nothing eventually moves on to easier targets. Not paying is not just the safe choice; it is the choice that actually protects you and makes the threat lose its grip.

WATCH OUT

Paying never buys silence — it marks you as someone who pays, and invites more demands. The money funds the people tormenting you. Do not pay, however frightening the threat.

4. Don't Engage, Don't Panic

The other two rules that protect you.

Alongside not paying, two companion rules complete your protection: do not engage, and do not panic. Not engaging means you stop communicating with the extortionist — you do not reply, argue, plead, explain, or try to reason with them. Any response, even an angry or pleading one, tells them you are reachable and affected, which encourages them. The silence of no response is powerful; it denies them the reaction and the engagement their scheme feeds on.

Not panicking is harder but just as important, because panic is exactly what the criminal is counting on to make you act against your own interest. The threats are designed to create a sense of catastrophe and urgency — 'I'll send this to everyone you know within the hour unless you pay now' — precisely to stampede you into paying before you can think or seek help. Recognizing the panic as a deliberate tool, rather than a true measure of your danger, helps you set it aside and respond with the calm steps that actually work.

Together, these three rules — don't pay, don't engage, don't panic — are your core response, and they are within your power even in a frightening moment. They may feel difficult when fear is screaming at you to make it stop, which is why it helps to have decided on them in advance and to lean on someone you trust to hold steady with you. The criminal's whole scheme assumes you will pay, engage, and panic. Doing the calm opposite of all three is how you defeat it.

GOOD TO KNOW

Three rules protect you: don't pay, don't engage, don't panic. The threats manufacture urgency precisely to make you act before you think. Calm, silence, and refusal take away their power.

5. Why the Fake Has No Real Power

Seeing through the threat.

It helps enormously to understand why a deepfake threat has so much less power than it feels like it does. First, if the image is AI-generated and fake, it is simply not real — it depicts something that never happened, and increasingly, people and institutions understand that such fakes exist and are not evidence of anything about you. The existence of convincing fakes, ironically, is becoming widely known, which undermines any fake's ability to truly shame or incriminate you.

Second, in the mass version of this scam, the criminal very often has nothing at all — no image, real or fake — and is bluffing to a long list of people, hoping a few will panic and pay. They may include a real detail about you, such as an old password from a data breach or your name and address, to seem credible, but a stolen detail is not proof they have any image. The frightening specifics are usually just bought data, deployed to make a hollow threat seem real.

Third, even in the rare case where some material exists, paying still does not protect you, and the response remains the same. In every version, the criminal's power comes not from what they actually hold but from your fear that they hold it and your dread of exposure. When you refuse to let that fear drive you, and you respond with the calm, correct steps, you take away the only real leverage they ever had. The threat is built of fear; starve it of fear, and it collapses.

GOOD TO KNOW

A fake image is not real and proves nothing, and in mass scams the criminal often holds nothing at all. Their power is your fear of exposure — refuse the fear, and the threat collapses.

6. Where the Images Come From

Understanding reduces the fear.

Knowing where these fake images come from helps demystify the threat and reduce its power to frighten. For the AI-generated kind, criminals typically take ordinary, innocent photos of a person — pulled from public social media, a profile picture, a shared photo — and use software to alter them into fake explicit or compromising images. You did not do anything to create the image; your ordinary public photo was simply taken and defiled by a computer, without your knowledge or consent.

This is important because it removes any sense that the image reflects on you or something you did. The FBI has warned publicly that criminals are using AI to turn people's ordinary online photos — including those of entirely innocent adults and, horribly, minors — into fake explicit content for harassment and extortion. The victims did nothing wrong; their images were stolen and altered. If this is happening to you, the shameful act is entirely the criminal's, and the fake depicts a lie, not you.

For the bluffing version, there is no image at all, just a threat built around scraps of data. Either way, understanding the source strips the threat of its moral weight: you are not being 'caught' at anything, because there is nothing real to catch. You are being lied to and threatened by a criminal who has either fabricated a falsehood or has nothing at all. Seeing that clearly is a large part of taking back your footing and meeting the situation with steadiness rather than shame.

GOOD TO KNOW

Fake images are made by stealing your ordinary, innocent photos and altering them with a computer — without your knowledge. The image is a lie about you, and the shame belongs entirely to the criminal.

7. It Is Not Your Fault

Setting down the shame.

I want to say this as plainly and gently as I can, because it is the heart of getting through this: it is not your fault. Whether the criminal has a fake image made from your innocent photos, or nothing at all, you have not done anything wrong, and you are the victim of a crime, not the author of a scandal. The shame these criminals try to make you feel is a weapon they aim at you, not a true reflection of anything about you or your character.

This matters because shame is exactly what the scheme runs on. The criminal is betting that you will feel so humiliated and afraid of judgment that you will pay in secret rather than tell anyone or seek help. Shame isolates you, silences you, and pushes you toward paying — all the things that help the criminal and harm you. Recognizing that the shame is manufactured and misdirected lets you set it down, which frees you to do the things that actually protect you: reaching out, reporting, refusing to pay.

So please be as compassionate with yourself as you would be with a dear friend in this situation. You would never tell a friend that a criminal's fake image or hollow threat was their fault, or that they should be ashamed; you would tell them they were wronged and that you were there for them. Offer yourself that same truth and kindness. The fault, the shame, and the wrongdoing all belong to the criminal. You are simply someone a criminal targeted, and you are going to be okay.

GOOD TO KNOW

The shame the criminal tries to make you feel is a weapon, not the truth. You did nothing wrong; you are the victim of a crime. Setting down the shame frees you to get help and stay safe.

8. What to Do, Step by Step

A calm checklist for right now.

Here is the clear, calm sequence of what to do if you are being threatened. You do not have to do it all at once or perfectly; just work through it steadily, and lean on someone you trust to help. These steps are drawn from the guidance of law enforcement and victim-support experts, and following them is how these situations are brought to an end.

- 1 Stop communicating with the extortionist — do not reply, pay, or engage any further.
- 2 Do not pay, no matter what they threaten or what deadline they set.
- 3 Save the evidence before blocking: screenshot the messages, note the account names, numbers, or profiles, and record what was threatened and demanded.
- 4 Do not delete your accounts or the conversation in a panic — the evidence matters for reporting.
- 5 Report it: to the FBI's Internet Crime Complaint Center at ic3.gov, and to the platform where it's happening.
- 6 Tell someone you trust — you do not have to carry this alone — and consider telling local police.

A note on order: save the evidence before you block or report, because once you block the account you may lose access to the messages, and the evidence helps the investigation. After you have the evidence, you can block the criminal and tighten your accounts. Throughout, remember the three rules — don't pay, don't engage, don't panic — and that reaching out for help is a strength, not a weakness. There are people whose job is to help with exactly this.

TIP

Save the evidence (screenshots, account names, what was threatened) **BEFORE** you block the account — blocking can cut off access to the messages investigators may need.

9. Reporting and Getting Help

The people and places ready to assist.

You do not have to handle this alone, and there are authorities and organizations ready to help with exactly this kind of crime. Reporting matters both for your own situation and because it helps investigators pursue these criminals, who often target many people. Even though it can feel frightening to tell anyone, the people who handle these reports are professionals who have seen many such cases and will treat you with respect and discretion, not judgment.

- The FBI's Internet Crime Complaint Center at ic3.gov is the main place to report extortion and deepfake crimes.
- Report the content and the account to the platform or app where it is happening; major platforms have processes for this.
- Your local police can take a report, which is useful documentation and appropriate especially if you feel unsafe.
- If the victim is a minor, contact the National Center for Missing & Exploited Children (NCMEC) and its 'Take It Down' service, which helps remove explicit images of minors; report to NCMEC's CyberTipline.
- Victim-support organizations exist for these situations and can offer guidance and emotional support.

If explicit fake images of you (as an adult) have actually been shared or you fear they will be, there are also services and newer tools aimed at helping remove such content from platforms, and the platforms themselves increasingly act against non-consensual and AI-generated explicit imagery. A victim-support organization or the authorities can point you to the current resources. The landscape of help is growing as awareness of these

crimes grows, and you are far from the first person to need it.

GOOD TO KNOW

For a minor who is targeted, contact NCMEC's CyberTipline and its Take It Down service right away — they specialize in getting explicit images of minors removed. For adults, the FBI (ic3.gov) and the platform are the first stops.

10. The Romance-Scam Doorway

How these threats often begin.

Many extortion cases begin through a different scam entirely: an online relationship. A criminal poses as a romantic interest or a friendly new contact, builds rapport over days or weeks, and steers the conversation toward intimate chat or requests for private photos or video. Once they have material — or even without it — they flip, revealing themselves as an extortionist and threatening to expose the victim unless paid. The warmth was a trap, and the shift to threats can be abrupt and shocking.

This pathway is worth knowing for two reasons. First, prevention: be cautious with online contacts who move quickly toward intimacy, who you cannot verify are real, or who steer toward private images, since this is a known setup for extortion. The same caution that protects against romance scams — never trusting an online-only relationship too far, never sharing compromising material with someone you have not verified in person — guards against this doorway. A video call is no longer proof a contact is genuine, given deepfakes.

Second, compassion for those caught this way: if an online relationship turned into extortion, the same truths apply — it is not your fault, you were deliberately manipulated by a criminal, and the response remains don't pay, don't engage, save evidence, and report. The shame around how it started is exactly what the criminal exploits to keep you silent and paying. Setting that shame aside and getting help is the way through, just as with any version of this crime. You were deceived by a predator, not undone by your own choices.

WATCH OUT

Be wary of online contacts who move fast toward intimacy or private images and can't be verified in person. This is a classic doorway to extortion — and a video call is no longer proof they're real.

11. Protecting Your Photos in Advance

Lowering the raw material for fakes.

While the threat is real for anyone, you can reduce your exposure by limiting how much of your image is publicly available for criminals to misuse, just as with voice cloning. You cannot and need not erase yourself from the world, and no amount of privacy guarantees immunity — but closing the easy doors makes you a harder target and is sensible prevention. The same privacy habits that guard against other AI misuse apply here.

- Set your social-media accounts to friends-only or private, so strangers cannot freely harvest your photos.
- Be thoughtful about posting lots of clear, forward-facing photos of yourself publicly.
- Ask friends and family not to tag or reshare your images publicly, and review your tagging settings.
- Never share intimate or compromising images with anyone you have not verified and deeply trust, and be aware even those can be misused.
- Help younger family members, who post the most photos, tighten their privacy — they are frequent targets.

These steps lower the supply of images a criminal could steal and alter, which genuinely reduces risk. But I want to pair them with reassurance, not fear: even if an image of you exists publicly, and even if a fake is made, the response and the outcome are the same — the threat has no real power when you refuse to pay, engage, or panic, and you get help. So tighten your privacy as sensible prevention, but do not lie awake over it; the defense that truly protects you is how you respond, not whether a photo of you exists somewhere.

TIP

Setting social accounts to friends-only lowers the photos a criminal can steal and fake. It's sensible prevention — but remember the real protection is how you respond, not whether a photo exists.

12. If It's Targeting a Young Person

What parents and grandparents must know.

This crime has tragically targeted young people, including teenagers, and every parent and grandparent should know about it, because the stakes for a frightened young person can be especially high. Criminals, often posing as a peer or a romantic interest online, manipulate a teen into sending an image or simply fabricate one, then threaten to send it to the teen's friends and family unless paid. The shame and panic a young person feels can be overwhelming, and tragically, some have been driven to despair before telling anyone.

The most protective thing is an open, judgment-free relationship where a young person knows, in advance, that if anything like this ever happens, they can come to a trusted adult immediately and will be met with help and love, never anger or blame. Tell the young people in your life, plainly and calmly, that this scam exists, that it is never their fault, that they should never pay, and that no mistake they could make online would ever make you love them less or refuse to help. That reassurance can be lifesaving.

If a young person is targeted, the response is the same — don't pay, don't engage, save evidence — plus specialized help: contact the National Center for Missing & Exploited Children through its CyberTipline and its Take It Down service, which is designed to help remove explicit images of minors, and involve law enforcement. And wrap the young person in support and reassurance throughout; their emotional safety is paramount. This is a crime against a child, and there are people dedicated to helping in exactly these cases.

WATCH OUT

Tell the young people you love, in advance: if anyone ever threatens them with an image, come to me immediately — you'll get help and love, never blame. That open door can be lifesaving.

13. The Bluff-to-a-List Version

Mass emails that have nothing on you.

A very common form of this is purely a bluff sent to huge lists of email addresses, and recognizing it can bring immediate relief. You receive an email claiming the sender has hacked your device, filmed you through your webcam, or has compromising footage, and demanding payment — usually in cryptocurrency — within a short deadline. To seem credible, the email may show you an old password of yours or your phone number, implying deep access. In reality, the sender has none of what they claim.

These emails are sent automatically to millions of addresses, with the personal details — like that old password — pulled from past data breaches that exposed such information publicly. The criminal has not hacked you, has no footage, and is simply gambling that a small fraction of recipients will be frightened enough by the accurate-looking detail to pay. The threatening technical claims are fabricated boilerplate, identical across countless victims. There is nothing real behind the menace.

The response is the easiest of all: do not pay, do not reply, and delete it, treating it as the empty bluff it is. If the email showed an old password, that is a sign that password appeared in a breach, so change it anywhere you still use it and turn on a second lock — not because the email is real, but as good general hygiene. You can report these to the FBI if you like, but mainly you can let go of the fear: this version is a hollow mass-mailing, and you are one of millions who received the identical lie.

GOOD TO KNOW

The 'I hacked your webcam, pay in crypto' email is a mass bluff with nothing behind it. The old password it shows came from a data breach, not a hack. Don't pay — delete it, and change that old password.

14. The Emotional Toll Is Real

Caring for yourself through it.

Even when you understand that the threat has no real power, being targeted by extortion is genuinely distressing, and it is important to acknowledge and tend to that. The fear, the violation, the shame the criminal tries to impose, the stress of the threats — these take a real emotional toll, and it is completely normal to feel shaken, anxious, angry, or low afterward. Please do not add to your burden by feeling you should simply 'get over it' quickly or handle it entirely alone.

Lean on people you trust. Telling a trusted friend, family member, or partner not only helps practically but breaks the isolation the criminal depends on and lightens the emotional weight of carrying it secretly. You will very likely find support and understanding rather than the judgment you fear, because the people who care about you will see clearly that you were wronged. If the distress is heavy or persistent, there is no shame in seeking support from a counselor or a victim-support service; these situations can be genuinely traumatic, and help is available.

Be patient and gentle with yourself as the feelings settle, which they will. The sharp fear fades as the threat proves hollow and time passes, and many people come through this not only recovered but with a hard-won sense of their own resilience. You faced a frightening, cruel thing and did not let it defeat you. That is something to hold onto. Your wellbeing matters most of all, far more than any criminal's empty threat, and tending to it is part of how you win.

GOOD TO KNOW

The emotional toll is real even when the threat is hollow. Lean on people you trust, and consider a counselor or victim-support service if the distress is heavy. Your wellbeing matters most.

15. Helping Someone Being Targeted

How to support a loved one.

If someone you love comes to you because they are being extorted this way, how you respond in that moment matters enormously — it may have taken great courage for them to tell you, overcoming the shame the criminal weaponized. Lead, immediately and sincerely, with calm, love, and zero judgment: 'I'm so glad you told me. This is not your fault. We're going to handle this together, and you're going to be okay.' That response is itself part of the rescue, because it breaks the isolation and shame the scheme depends on.

Then help them follow the calm steps: don't pay, don't engage, save the evidence, and report to the authorities. Take on the parts that overwhelm them, help them gather the evidence and make the reports, and stay with them through it. Steadiness is the great gift here — your loved one is frightened and may be in a spiral of shame and panic, and your calm confidence that this is a known, beatable crime helps them find their own footing. Reassure them, repeatedly, that the fault and shame belong to the criminal, not to them.

Watch especially for signs of deep distress, particularly in a young person, and take them seriously. If someone seems to be in crisis or despair, stay with them, keep them talking, and connect them with help — a trusted adult, the authorities, a counselor, or a crisis line. Your presence and your unconditional support can be genuinely lifesaving in these moments. Above all, make sure your loved one knows they are not alone, that they did nothing wrong, and that this frightening thing will pass with your help.

GOOD TO KNOW

If a loved one tells you they're being extorted, your first words matter most: 'I'm so glad you told me — this is not your fault.' Calm, unconditional support breaks the shame the scheme runs on.

16. Questions People Ask Me

The ones that come up, gently answered.

What if the image looks completely real? Convincing fakes are exactly what AI now makes easy, so realism is not evidence the image is genuine or that it reflects anything you did. And whether it is a flawless fake or the criminal is bluffing, the response is the same: don't pay, don't engage, save evidence, and report. Realism increases the fear but changes nothing about the right steps.

If I just pay this once, won't they go away? No. Paying marks you as a payer and brings more demands, every time. There is no version where paying buys lasting silence. Not paying is both the safe choice and the one that most reliably ends it, because an extortionist who gets nothing moves on.

Isn't it too embarrassing to report or tell anyone? The people who handle these reports and the people who love you will see you as the victim of a crime, not as someone to judge. The embarrassment is the criminal's weapon; reporting and telling someone is how you take your power back. You are far from the first to face this, and help is given with respect and discretion.

They had my real password — doesn't that mean they hacked me? Usually not. Old passwords and personal details are widely exposed in data breaches and used to make hollow threats look credible. A real detail is not proof they have any image or access. Change that password and turn on a second lock as good hygiene, and treat the threat as the bluff it almost certainly is.

17. A Note on Prevention

Sensible habits, without fear.

While the most important message is how to respond, a few preventive habits lower your risk and are worth adopting calmly, without letting them become a source of anxiety. These overlap with general good digital safety, so you may already be doing much of this. Think of them as closing easy doors, not as building a fortress against an inevitable attack.

- 1 Keep social-media accounts private, limiting who can see and harvest your photos.
- 2 Be cautious with online-only relationships, and never share intimate images with someone unverified.

- 3 Turn on a second lock (two-step verification) on your important accounts, so they're harder to hack.
- 4 Keep your devices updated, and be wary of links and downloads that could give someone access.
- 5 Talk openly with family, especially young people, so everyone knows this exists and knows to come to you.

These habits make you a harder target and are simply good practice. But I will close the prevention point with the same reassurance that runs through this whole guide: even if someone does target you, the threat has no real power when you respond correctly. So adopt sensible prevention, but carry it lightly. The knowledge that you know exactly how to defeat this crime — don't pay, don't engage, don't panic, save evidence, get help — is a far greater protection than any worry, and it lets you live without fear.

GOOD TO KNOW

Adopt sensible prevention lightly, without anxiety. The greatest protection isn't preventing every possible attack — it's knowing exactly how to defeat this crime if it ever comes.

18. You Will Get Through This

A steady, hopeful close.

I want to end where I began, with steadiness and hope, because if this is happening to you, that is what you most need to hear. This is a frightening, cruel crime, but it is one that is understood, that has clear and effective responses, and that people face and defeat regularly. You are not the first, you will not be the last, and there is a well-worn path through it that leads out the other side. The fear you feel right now is real, but it is temporary, and it is not a measure of true danger.

Hold onto the core truths: it is not your fault, the threat's power is your fear and nothing more, you must not pay or engage, and you do not have to face it alone. Save the evidence, report it, tell someone you trust, and lean on the authorities and support services whose job is to help with exactly this. Each of those steps takes a little of the power back from the criminal and returns it to you, where it belongs.

And please remember you can reach out for help, including to me, at any point. If the technology side feels overwhelming — gathering evidence, tightening your accounts, making a report online — that is exactly the kind of thing I can calmly help a neighbor with, without judgment and in confidence. You have faced something hard and handled it by

reading this and taking the steps. That is strength. You are going to be all right, and there are people, me among them, ready to help you get there.

GOOD TO KNOW

This is understood, common, and beatable. It is not your fault, the threat's only power is your fear, and you are not alone. You will get through this — and help is available the whole way.

19. 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.

20. When to Just Call Me

A calm second opinion costs you nothing.

If something about a threat to release a fake or doctored image or video of you or a loved one 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.

21. 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.

If this is happening to you or someone you love, please know it is not your fault, you are not alone, and help is available. Do not pay, save the evidence, and reach out — to the authorities, to someone you trust, and to me if the technology feels overwhelming. You will get through this.

CHEAT SHEET

Everyday Cheat Sheet

The three rules

- Don't pay — it only brings more demands.
- Don't engage — no replies, no pleading.
- Don't panic — urgency is a manufactured tool.

What to do

- 1 Save the evidence (screenshots, accounts, threats) before blocking.
- 2 Don't delete accounts or messages in a panic.
- 3 Report to the FBI at ic3.gov and to the platform.
- 4 For a minor: contact NCMEC's CyberTipline and Take It Down.
- 5 Tell someone you trust — you're not alone.

Remember

The image is usually fake or nonexistent, it is not your fault, and the threat's only power is your fear. Help is available, with respect and no judgment.

GOOD TO KNOW

This is a sensitive topic. If you're in distress, please reach out to someone you trust or a crisis resource right away — you deserve support, and you will get through this.

AT A GLANCE

A Picture to Follow Along

Why the Threat Is Hollow

The criminal's only real weapon is your fear.



Refuse the fear - and the threat loses all its power.

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

AT A GLANCE

A Second Look

What to Do, Calmly

Three rules, then steady action.

- 1 A threat demands money over an image
- 2 Don't pay - it only brings more demands
- 3 Don't engage, don't panic
- 4 Save the evidence before blocking
- 5 Report to the FBI (ic3.gov) and the platform
- 6 Tell someone you trust - you're not alone

It is not your fault, and help is available with no judgment.

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.