

Google isn't calling to charge you

The calls, letters, emails and texts that pretend to be Google or your domain company, how to tell them from the real thing, and what to do if one already got you.

Google does phone businesses. A recorded voice might ring to check your hours or to book a customer in, and now and then it's a person. But Google says it will never ask for payment, credit card information, or account passwords, it won't guarantee you a special spot, and the listing itself is free.

This guide is about the calls, letters and emails that don't fit. A recorded voice says your listing is about to come down. An envelope looks like the renewal for your web address, from a company you've never dealt with. An email offers to put you first on Google.

They're aimed at whoever answers the phone, opens the post and pays the bills. In a small trade business that's often one person. Every section ends with something to do this week, and none of it costs anything.

01 The call: "This is Google, there's a problem with your listing"

The real calls are about small things. Google's help page says they're for booking a customer in, checking a wait time, a price or what's in stock, or checking your hours. A real one tells you it's Google and why it's calling (Google). Answering one "does not affect your account standing."

Add one more to the list of things Google won't do on a call: ask you to sign up for a service. And in Google's words: "If a caller asks for money to keep your business on Google, it is not a call from Google" (Google).

The fake calls run to a few scripts. Google's Business Profile community guide, written by Product Experts rather than Google staff, lists the common ones. Someone "with Google" offers to set up or boost your profile for a fee. Someone threatens to take the profile down unless you pay. Or there's an emergency: the number on your listing is wrong and sending work to another company, and they need your password or payment details to fix it.

The same guide says Google doesn't hire outside companies to work with business owners on its behalf, so "we work with Google" is the warning. Google's own fraud page says the same about callers who say they work "with Google" or "for Google".

The name on your screen proves nothing. Scammers fake their numbers, and the FTC's advice is plain: "don't trust caller ID."

And if a recorded voice says to press 1 to be taken off the list, don't. Google: "Do not press any buttons even if the voice prompt tells you to. Pressing buttons might lead you to more suspicious calls" (Google). Hang up.

If Google's own automated calls bother you, you can turn them off in your profile, or say "Please stop calling my business" on the call. A person from Google may still ring now and then to confirm your details.

WHAT TO DO THIS WEEK

- Write one sentence on a card by the phone: Google won't ask for money, a card number or a password. If the caller does, hang up.
- Tell anyone else who answers your phone the same thing, today.
- Never press a number a recorded voice asks for.
- Never claimed your profile? The community guide says pitches to set your profile up for a fee go after exactly those businesses. Claim it yourself; the sixty-seconds guide shows where.
- To stop Google's automated calls: Business Profile, More, Business Profile settings, Advanced settings.

A real call from Google asks about your hours. A fake one gets round to your card number.

02 The letters and invoices: the bill for something you never ordered

Some arrive on paper, made up to look like a bill. The FTC describes phony invoices that look like something you ordered: "They hope the person who pays your bills will assume the invoices are real and make the payment." Its 2026 alert names the usual subjects: tech support, domain registration, and search engine optimization, some of them stamped "past due" to hurry you along.

The domain letter has been around a long time. In a 2010 case, the FTC described invoices made to look as if they came from the business's own domain company. They listed the business's real web address, or a near copy with ".org" in place of ".com", and billed for an annual "WEBSITE ADDRESS LISTING" with search optimization thrown in. Most of the people who got them were led to believe they had to pay to keep their domain.

Genuine renewal reminders come from the company you registered the domain with. For a .com and most other generic endings, ICANN's rules make that company send at least two: one about a month before it expires, one about a week before. ICANN itself never requests payment of fees from domain owners.

Directory listings work on the phone first. A call offers a "free" listing, or just wants to "confirm" your details, and later a big bill turns up, sometimes with a recording of that call to pressure you into paying. The FTC's answer is six words: "If you didn't agree, don't pay."

Then there's the letter dressed as government, with an agency name built from words like United States, business regulation and trademark, warning of fines if you don't respond fast.

How they want to be paid is a tell. Wire transfer, gift cards, cryptocurrency: the FTC says "Don't pay anyone who demands payment this way."

And if goods you never ordered turn up in the post, the FTC says you have a legal right to keep them and use them, without paying.

WHAT TO DO THIS WEEK

- Find out who your domain is registered with and when it renews. Log in to that account, or type your web address into ICANN Lookup. Write the company name and the date down.
- Put that note where whoever opens the post will see it. A letter about your domain from any other company goes in the bin.
- Agree one rule with whoever pays the bills: nothing gets paid that you can't match to something you ordered.
- Anything that wants paying by wire, gift card or crypto doesn't get paid.
- While the bank statement is open, leak 7 of the leaks guide is the listing that renews every year without anyone deciding it should.

If nobody can remember ordering it, assume nobody did.

03 The emails and texts: first place on Google, bad reviews gone, "renew now"

The same tricks come by email and text, with a link to click instead of a number to call. Start with SEO. Google's own guide to hiring help with search says to be wary of firms that email you out of the blue, and adds: "Amazingly, we get these spam emails too." It also says, flatly: "No one can guarantee a #1 ranking on Google." And it says to beware anyone who claims a "special relationship" with it.

"We can remove your bad reviews" is the next one. The FTC says scammers claim they can replace negative reviews or add positive ones, and that posting fake reviews is illegal. What you can do is report a review yourself, from your own profile. Google is clear that "only those that violate Google policies are eligible for removal," and if you disagree with its decision you get one appeal. No outside company can get you more than that. Replying to the bad ones is a better use of the time.

A fake invoice by email can be after more than the payment. The FTC says some are phishing, designed to get into your business's data and networks.

Domain emails do the same. ICANN has warned about emails that offer a renewal and say "click here" to renew online "at attractively low rates." ICANN does not email domain owners about

managing their domains at all, and its advice for any of these is to contact the company you registered with, directly.

Texts that claim to be Google get the same treatment. Google says it will never ask you for private or sensitive information, and if a text comes from an unverified account, don't reply or click anything.

WHAT TO DO THIS WEEK

- Delete any email that promises you first place on Google.
- Got an email about your domain, your listing or an invoice? Close it, and log in to the account yourself.
- A review that breaks Google's rules: report it from your own profile.
- Forward phishing emails to reportphishing@apwg.org and scam texts to 7726.

The link is the scam. Go round it.

04 How to check what's real: hang up, then go to the account yourself

One habit covers everything above. Don't act on the call, the letter or the email. Hang up, close it, and contact the company through a number or a website you already had.

Google, the FTC and ICANN all give that advice. The FTC's version, written about fake government letters, fits every case: "Don't use any websites or phone numbers listed in the letter."

Take your time doing it. The rush is part of the scam: scammers "want you to act before you have a chance to check out their claims." And before you pay any company you haven't paid before, search its name with "scam", "review" or "complaint" after it.

Then check who already has a key. Your profile has a page called People and access that lists every owner and manager. As the owner you can remove anyone on it. Google's tip is that each person gets their own Google account, so nobody ever needs your password.

For the domain, ICANN suggests two-step sign-in where your domain company offers it, and a "registrar lock", which helps stop anyone changing, moving or deleting the domain. It also suggests the account use a different email address from the one on the domain itself.

WHAT TO DO THIS WEEK

- Open your profile: Business Profile, More, Business Profile settings, People and access. If there's a name you don't know, find out why it's there before you remove it.
- Turn on two-step sign-in for the Google account that owns the profile, and for your domain account.
- Ask your domain company for a registrar lock.

- Save your domain company's real phone number and login page in your phone, so you never need the one printed on a letter.
- Tell everyone who answers your phone or opens your post the rule.

A real problem will still be there when you log in.

05 If you've already paid, or handed over a password

It happens to careful people. What matters now is speed, and the FTC's steps are short.

Paid by card: call the number on the back of it, report it and ask for a refund. The FTC adds that federal law protects you from unauthorized use of your card.

If it went by bank transfer or Zelle, report it to your bank straight away and ask them to reverse the payment. A payment app, the same: report it to the app straight away.

Wire, gift cards and crypto are the hard ones. Contact the company you used to send it, straight away, and be ready for bad news. The FTC's own words are "your money might be gone already," and it still says it's always worth asking.

Gave a password: change it now, and anywhere else you used the same one, then turn on two-step sign-in. Let someone onto your computer: update your security software, run a scan, delete what it flags, change your passwords.

After that, check the two things this guide keeps coming back to: the People and access list on your profile, and the contact email and settings on your domain account. Someone with your domain login can point your domain wherever they like.

If a directory company plays you a recording of the call where you "agreed", the FTC warns that happens, and its advice stands: if you didn't agree, don't pay.

WHAT TO DO THIS WEEK (IF IT APPLIES)

- Call your card company or bank today, not tomorrow.
- Change the password, then turn on two-step sign-in.
- Check People and access on your profile.
- Report it. The addresses are below.

The phone call to the bank today beats the careful one next week.

06 Where to report it

The FTC says a report "can help stop the scam." Worth a bookmark.

- **The FTC**, for any of it: ReportFraud.ftc.gov

- **The Do Not Call Registry**, for calls that keep coming: donotcall.gov or 1-888-382-1222
- **The FCC**, for robocalls and unwanted texts: consumercomplaints.fcc.gov
- **Google**, for a caller who says they're from Google or work with it: its report form. It asks for the caller's company and contact details, and anything they sent you afterwards, so keep those.
- **Phishing emails**: forward them to reportphishing@apwg.org
- **Scam texts**: forward them to 7726
- **Emails claiming to be ICANN**: globalsupport@icann.org
- **Your state attorney general**: the FTC points to NAAG, which lists every one.

Every report adds to what the FTC builds its cases from.

WHERE TO START

If you do one thing from this guide: write down who your domain is registered with and when it renews, and check the People and access list on your profile. If you do two: that, and give whoever answers the phone and pays the bills the rule. Google won't ask for money, a card or a password. Nothing gets paid that nobody ordered. Anything urgent gets checked by logging in yourself.

None of it needs a website.

Hang up. Log in. Pay only what you ordered.

Everything above depends on knowing whose name your domain is in and who can log in to your listing. If someone else built your site, they may have set it up and never told you. Whoever built it should be able to say, in one sentence, whose name the domain is in and what it costs to take it with you. Here's mine.

On my monthly plan I register your domain and pay the renewals, so it's in my name while you're with me. If you leave and want to take it, you pay me what I last paid to renew it, the actual cost including tax and fees, with nothing added on top, and it's transferred to you. I don't make money on domains and I won't hold one hostage. With a one-time build you register it in your own name from the start. It's all on the pricing page and in the terms.

The free check I offer is for your website. Send it to me and I'll test your contact form and your phone links, and send you a short list of fixes within two business days. Free, and it obliges you to nothing.

Written by JT Creeden at RedHorseWebDev, who builds websites for small businesses anywhere in the US. The whole guide is free to read at redhorsewebdev.com/learn — this PDF is just easier to keep.