



An Extended Guide · No. 1934

Fake "Microsoft 365 Renewal" Emails & Too-Cheap License Keys

Tell a real renewal notice from a
scam, and why bargain keys stop working

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! The one rule that defeats these scams

Never click a link or call a number in an email that says your Office is expiring. Instead, check your real account yourself at account.microsoft.com. That single habit stops nearly every one of these tricks cold.

Spotting the fake renewal, avoiding the fake bargain

Scammers love Microsoft 365 because so many people pay for it. They send fake 'your subscription is expiring' emails to frighten you into clicking, and they sell too-cheap 'license keys' that stop working. This guide helps you see through both.

I'm Bill, from Bill's Home Tech in Portage County. I've helped many folks who got a scary renewal email or bought a bargain key that died. The good news: once you know the tells, these scams become almost easy to spot.

We'll go gently but plainly. By the end you'll know how to tell a real renewal notice from a fake, why cheap keys fail, and exactly what to do when a suspicious message lands.

The whole guide, on one page

If you remember only these, you're well protected.

- ❑ Real renewal info lives in your account — check it yourself at account.microsoft.com, not via an email link.
- ❑ Scam emails use fear and urgency: 'expires today,' 'act now,' 'you'll lose your files.'
- ❑ Never click links or call phone numbers in an unexpected 'renewal' email.
- ❑ Microsoft won't ask you to pay by gift card, wire, or over the phone with a stranger.
- ❑ Office for a tiny fraction of the real price is almost always a dead or stolen key.
- ❑ When in doubt, don't act — check your real account or ask someone you trust.

✓ Fear and urgency are the tell

Real companies don't panic you. If a message about your subscription makes your heart race and demands you act this instant, that feeling is the scam working.

Why scammers love Microsoft 365

Understanding why these scams exist helps you expect them and stay calm when one arrives.

Millions of people pay Microsoft a yearly fee, so a scammer who sends out a fake 'your subscription is expiring' email knows a good share of recipients really do have a subscription — making the lie believable. And because folks worry about losing access to Word or their files, fear does the scammer's work.

The cheap-key scams work on the opposite emotion: the pleasure of a bargain. Office isn't cheap, so 'Office for \$15, today only!' is tempting. But legitimate software doesn't sell for pocket change, and these keys are stolen, shared, or simply fake — destined to stop working.

✓ They play on fear and on bargains

Two emotions power these scams: fear of losing your Office, and the thrill of a deal. Notice when a message is pulling either lever, and slow down.

What a fake renewal email looks like

These emails follow a pattern. Once you've seen it, you'll recognize the next one instantly.

- **Alarming subject:** 'Your Microsoft 365 has expired,' 'Final notice,' 'Action required.'
- **Urgency:** 'Renew within 24 hours or lose your files,' a countdown, a looming deadline.
- **A big button or link:** 'Renew Now,' 'Update Payment' — which leads to a fake page that steals your details.
- **A phone number to call:** leading to a fake 'support' person who'll ask for payment or remote access.
- **Odd details:** slightly wrong logos, awkward wording, an unfamiliar sender address behind a friendly name.

Any one of these is a warning; several together mean it's almost certainly a scam. The goal is always the same — to get you to click, call, or pay in a panic before you stop to think.

! The button is the bait

That 'Renew Now' button is the whole trap. It leads to a lookalike page built to capture your password and card. Never click it — go to your real account instead.

How to check your real subscription

Here's the habit that makes you scam-proof: ignore the email and check your actual account yourself.

- ❑ Open your web browser and type account.microsoft.com yourself (don't click an email link).
- ❑ Sign in with your real Microsoft account.
- ❑ Click 'Services & subscriptions.'
- ❑ There you'll see the truth: whether you have a subscription, when it renews, and the real cost.
- ❑ If the email's claim doesn't match what you see here, the email was fake.

This works every time because it bypasses the scammer entirely. Whatever a frightening email claims, your real account page tells you the actual situation — and it's the only source you should trust about your subscription.

★ I'll show you your real account page once

Learning to check account.microsoft.com yourself is the single best defense against renewal scams. I'm glad to walk you there once so it's familiar forever. Call (330) 200-8042.

Telling a real notice from a fake one

Microsoft does send genuine reminders. Here's how the real ones differ from the scams.

A real notice	A scam
Calm, informational	Frightening, urgent
No gift-card demands	Gift cards, wire, odd pay
Matches your account	Doesn't match reality
No pressure to call	Pushes a phone number

Even with a genuine reminder, the safe move is the same: don't act from the email itself — go to your account page and handle any real renewal there. That way it doesn't matter whether a given email is real or fake; you always act from the trustworthy source.

✓ Treat every renewal email the same way

You don't have to judge each email perfectly. Whether it looks real or fake, go to your account page to check and renew. Consistency beats case-by-case guessing.

Why too-cheap license keys stop working

Now the other scam: those 'Office for \$15' deals. Here's why they're a false economy.

A product key is the code that activates Office. Legitimate keys cost real money because the software does. When you see Office offered for a tiny fraction of the normal price, that key is almost always one of three bad things: stolen, shared with hundreds of other buyers, or a type meant for businesses or schools that isn't licensed for you to buy.

These keys may activate at first, then stop working weeks or months later when Microsoft detects the abuse and deactivates them. You're left with non-working Office and no refund — having paid a stranger who's long gone. The bargain was never real.

! A dead key costs more than a real one

Spending \$15 on a key that dies in a month, then having to buy the real thing anyway, costs more than just buying it right the first time — plus the aggravation.

Where the fake bargains show up

Knowing where these too-cheap keys appear helps you steer clear of them.

- **Auction and marketplace listings** offering 'genuine Office, lifetime, \$19.'
- **Random websites** advertising steep discounts you've never heard of, often with countdown timers.
- **Email and pop-up ads** promising cheap keys with urgent 'today only' pressure.
- **Social media deals** shared by accounts you don't know.

The common thread is a price far below everyone else's and a seller you have no reason to trust. Real Office is sold by Microsoft and by known stores at prices in the same ballpark as each other — not at a tenth of the cost from a stranger.

✓ Buy only from Microsoft or a store you know

The safe sources are Microsoft's own site and trusted retailers — a big-box store, a warehouse club, a reputable online shop. Anything wildly cheaper is a warning, not a win.

The 'support call' version of the scam

Some of these scams move to the phone, which can feel even more convincing. Here's how that one works.

A fake renewal email (or a pop-up) gives a phone number for 'Microsoft support.' Call it and a friendly-sounding person offers to 'help with your renewal' — then asks to remotely connect to your computer, or for your card details, or has you buy gift cards to pay. All of it is the scam.

Real Microsoft support doesn't reach you through a number in a scary email, won't ask for gift cards, and won't cold-call to fix your subscription. If you're ever on such a call and feel pressured, it's completely fine to simply hang up — you owe a scammer nothing, not even politeness.

! Never let a 'support' caller into your computer

If someone from an email or pop-up wants to remotely connect to your computer or have you buy gift cards, it's a scam. Hang up. Our tech-support-scam guide covers this in depth.

Two kinds of readers, two sets of needs

These scams come at you two ways. Knowing both keeps you ready for whichever arrives.

If it's a scary 'renewal' message

An email, text, or pop-up warning your Office is expiring and pressing you to act now. The emotion it's pushing is fear.

- Don't click links or call numbers in it.
- Go to account.microsoft.com yourself to see the truth.
- Watch for urgency, odd pay methods, and lookalike pages.
- Delete it once you've confirmed your account is fine.

If it's a too-good bargain

A listing or ad offering Office far below the normal price. The emotion it's pushing is the thrill of a deal.

- Remember: real Office isn't sold for pocket change.
- Buy only from Microsoft or a store you recognize.
- Expect bargain keys to stop working — they're stolen or shared.
- A dead key plus buying the real one costs more in the end.

★ Got a message or deal you're unsure about?

Before you click, call, or buy, run it by me. Forward me the email or describe the deal at (330) 200-8042 and I'll tell you plainly if it's a scam. No charge for a gut check.

What to do when a scam email arrives

You've spotted a fake renewal email. Here's the simple, safe way to handle it.

- ❑ Don't click anything in it — no links, no buttons, no phone numbers.
- ❑ Don't reply, and don't open any attachment it carries.
- ❑ If you're unsure it's fake, check your real account at account.microsoft.com separately.
- ❑ Mark it as junk or spam, or simply delete it.
- ❑ If it's convincing, you can report it to your email provider as phishing.

That's the whole response: don't engage, verify independently if needed, and discard. You don't have to do anything clever — the power is simply in not taking the bait.

✓ Not acting is the winning move

With these scams, doing nothing — not clicking, not calling, not paying — is exactly the right action. The scam only works if you respond.

If you already clicked or paid

If you fear you've already fallen for one, don't panic and don't be embarrassed — act calmly on these steps.

- **If you entered your password** on a fake page: change your Microsoft account password right away at the real account.microsoft.com, and turn on extra sign-in security.
- **If you gave card details**: call your bank or card company, report it, and watch for unexpected charges.
- **If you bought gift cards**: contact the gift-card company immediately — occasionally funds can be stopped if you act fast.
- **If you let someone into your computer**: disconnect from the internet and get it checked by someone you trust.

These things happen to sharp, careful people — the scams are designed to fool anyone. The sooner you act, the more you can limit any harm. And there's no shame in it; the shame belongs entirely to the scammer.

★ Think you got caught? Call me

If you've clicked, paid, or let someone in, call me at (330) 200-8042. We'll calmly go through the steps to secure your account and computer. No judgment, ever — just help.

Common mistakes, and how to avoid them

A few understandable reactions are exactly what the scammers count on. Here's how to resist them.

- **Acting fast out of fear** — the urgency is manufactured; real matters give you time.
- **Clicking the email's link to 'check'** — go to your account page yourself instead.
- **Trusting a phone number from the email** — it leads to the scammer, not Microsoft.
- **Chasing a bargain key** — real Office isn't that cheap; the key will die.
- **Being too embarrassed to ask** — a quick check with someone you trust costs nothing.

✓ **Slow down — that's your superpower**

Every one of these scams needs you to hurry. The simple act of slowing down, and checking separately, defeats nearly all of them.

Making your account harder to crack

Beyond spotting scams, a couple of settings make your Microsoft account much safer even if a password slips out.

Turn on two-step verification (also called two-factor) for your Microsoft account. Then, even if a scammer gets your password, they still can't sign in without a code sent to your phone. It's the single strongest protection, and it's free — set up once at account.microsoft.com under Security.

Also use a strong, unique password for your Microsoft account, not one you reuse elsewhere. Our password guides walk through making this easy with a password manager. Together these mean a stolen password alone can't open your account.

★ I'll set up two-step security with you

Two-step verification is the best scam insurance there is, and it's quick to set up. I'm glad to do it with you so your account is protected even if you ever slip. Call (330) 200-8042.

You're smarter than these scams

If these schemes have worried or caught you before, please don't feel foolish — feel prepared.

These scams are professionally designed to fool intelligent, careful people; getting a jolt of fear from a convincing email is human, not naive. What matters is the simple habit you now have: don't act from the message, check the real source. That habit beats even the slickest scam.

You don't need to be a computer expert to be safe here. You just need to remember to slow down and verify — and you already do. That makes you a hard target, which is exactly what you want to be.

★ And you've always got a backstop in me

Whenever a message makes you uneasy, I'm a phone call away for a free gut check. Knowing that is its own kind of protection. Call or text (330) 200-8042.

Questions to ask yourself

When a renewal message or a deal appears, these questions settle it.

Q: Is this message trying to rush me?

Urgency is the scammer's tool. A real matter gives you time; manufactured panic is a red flag.

Q: Am I about to click a link or call a number from the message?

Don't. Go to account.microsoft.com yourself to check anything about your subscription.

Q: Does this price seem too good to be true?

Then it is. Real Office isn't sold for a few dollars by a stranger.

Q: Would it hurt to check with someone first?

Never. A two-minute gut check with a trusted person or with me beats a costly mistake.

✓ If it rushes or it's too cheap — stop

Two instincts cover most of it: a message that rushes you, or a price that's too cheap. Either one means stop and check.

A few more worth answering

These come up often with renewal scams.

Q: Does Microsoft email me about renewals?

It may send genuine reminders, but it won't threaten you, demand gift cards, or rush you. Either way, check and renew at your account page, not via the email.

Q: How can I tell if my subscription is really expiring?

Sign in at account.microsoft.com and open 'Services & subscriptions.' That page shows the real renewal date and cost — the only source to trust.

Q: Why did my cheap Office key stop working?

Because it was stolen, shared, or not licensed for individual sale. Microsoft deactivates such keys, leaving you with non-working Office and no refund.

Q: Is it safe to call the number in the email?

No — it leads to the scammer, not Microsoft. Real support is reached through Microsoft's official website, never a number in a scary email.

★ Unsure about a message?

Forward it to me or describe it at (330) 200-8042. Telling real from fake is quick for me, and I'm always glad to spare you a scam.

The whole thing, recapped

Here's your protection as a short, memorable routine.

- ❑ Never click links or call numbers in a 'renewal' message.
- ❑ Check your real subscription at account.microsoft.com yourself.
- ❑ Treat urgency, gift-card demands, and pressure as scam tells.
- ❑ Buy Office only from Microsoft or a store you trust — never a bargain key.
- ❑ Turn on two-step verification for your Microsoft account.
- ❑ Unsure? Don't act — check with someone you trust first.

Follow that and both the fake-renewal and cheap-key scams lose their power over you. The scammers need your haste and your trust; give them neither and they've got nothing.

✓ Check the source, not the scare

The whole defense in five words: check the source, not the scare. Your real account page always tells the truth.

Common Questions

The questions I hear most about renewal scams and cheap keys.

Q: How do I know if a 'Microsoft 365 renewal' email is real?

Don't judge the email — check your actual account at account.microsoft.com yourself. Scam emails use fear and urgency, push links and phone numbers, and sometimes demand gift cards; real notices do none of that.

Q: What should I do with a suspicious renewal email?

Don't click, call, reply, or open attachments. Verify your subscription separately at your account page, then mark the email as junk or delete it.

Q: Why do cheap Office keys stop working?

Because they're stolen, shared among many buyers, or not licensed for individual sale. Microsoft deactivates them, so you lose both the key and your money.

Q: Where should I buy Office safely?

From Microsoft's own website or a trusted retailer — a big-box store, warehouse club, or reputable online shop. Avoid any 'deal' far below the normal price.

★ Want a trusted second opinion?

A free gut check before you click, call, or buy can save you real money and worry. Call or text me at (330) 200-8042 anytime a message or deal seems off.

The bottom line

Here's the heart of it in a few sentences.

Fake 'renewal' emails use fear to make you click a link, call a number, or pay in a panic — so never act from the message; check your real subscription at account.microsoft.com yourself. Too-cheap Office keys are stolen or shared and will stop working — so buy only from Microsoft or a store you trust.

Add two-step verification to your account, slow down whenever a message rushes you, and keep a trusted person (or me) in mind for a quick gut check. With those habits, these scams simply bounce off you.

✓ Slow down, check the source, buy from the real place

That's the entire defense. The scammers need haste and trust; deny them both and you're safe.

One more thought, for your peace of mind

A closing word, because these scams prey especially on conscientious people.

If you're the kind of person who pays bills on time and doesn't want to lose access to anything, scammers count on that very decency — the worry that you might have missed a payment. Knowing that the worry itself is the bait turns your conscientiousness back into a strength.

So the next time a 'your Office is expiring' message tries to hurry you, you'll feel the tug, recognize it for what it is, and calmly check your real account instead. That's not being fearful — that's being wise, and it keeps your money and your files exactly where they belong.

★ Here whenever you need a steady voice

A suspicious email, a tempting deal, or a worry that you slipped — call or text me at (330) 200-8042. We'll sort it out calmly, together.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made spotting fake renewal emails and cheap-key scams feel a little less daunting and a lot more doable. Keep it in a drawer with your other home papers, come back to a page whenever you need it, and don't worry about memorizing anything.

When you'd rather have a hand, that's exactly what I do. I come to your home, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site — installing Office, sorting out a sign-in, setting up a document — I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

Real Notice vs. Scam

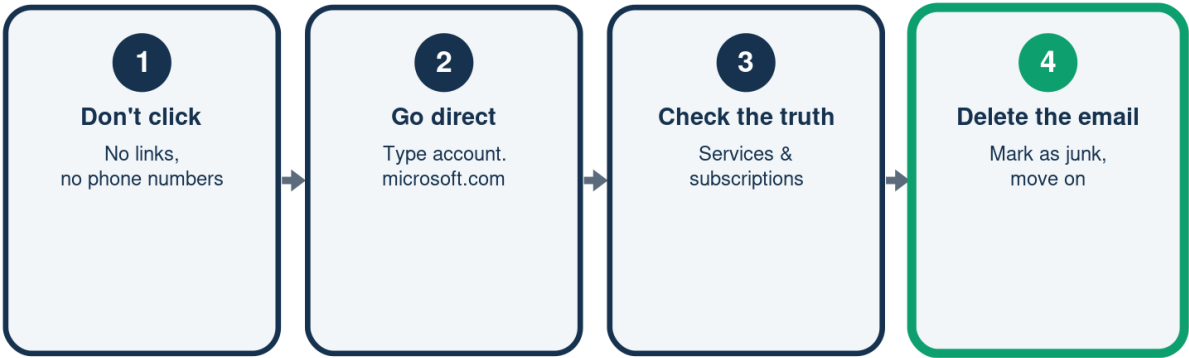
How to tell them apart

	Real	Scam
Tone	Calm	Frightening
Timing	No deadline panic	'Act now!'
Payment	Normal	Gift cards, wire
Matches account	Yes	No

Whichever it is, check and renew at your account page -- not the email.

When a 'Renewal' Email Arrives

The safe four steps



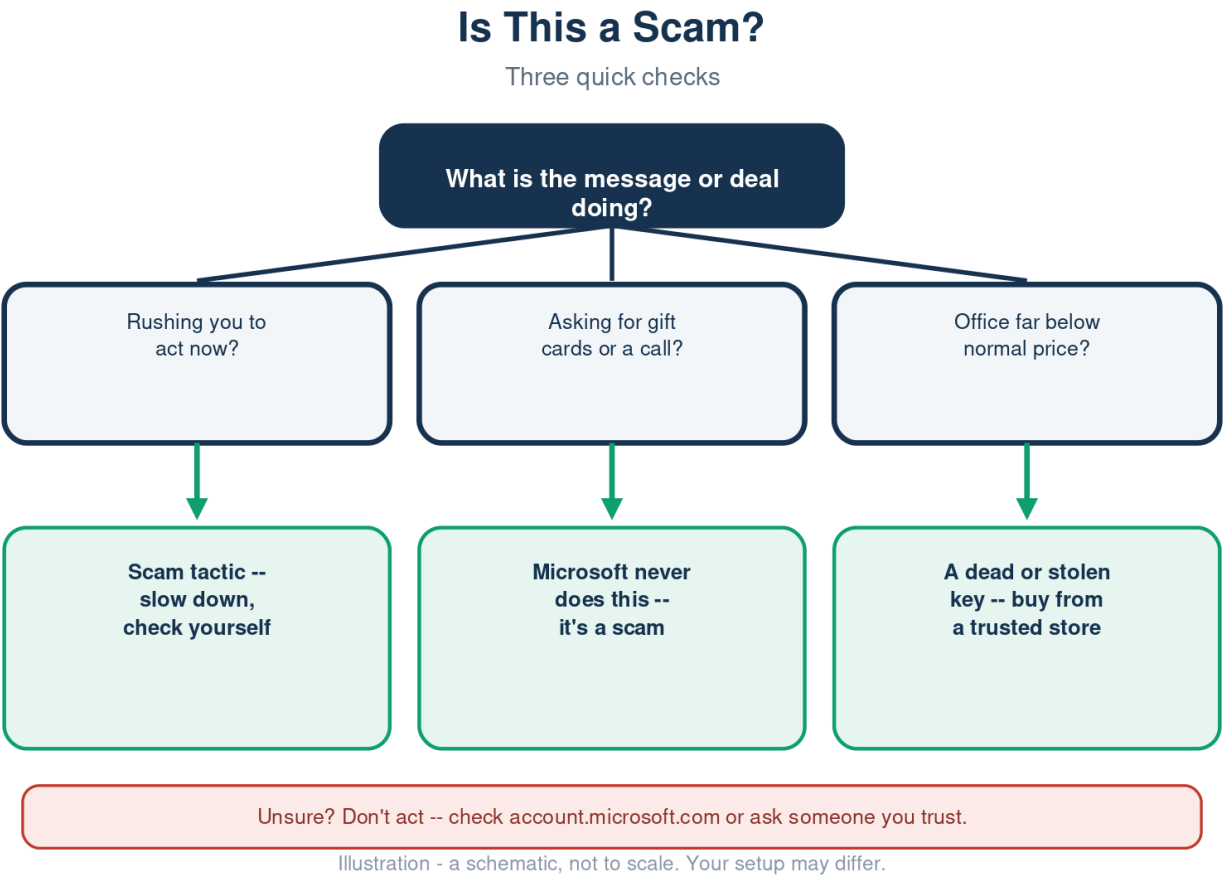
Check the real source yourself -- the email is never the place.

Why Cheap Keys Fail

What a bargain key really is

	The 'deal'	The reality
\$15 Office	Stolen or	shared key
Works at first	Then gets	deactivated
'Lifetime'	Dead in	weeks or months
No refund	Seller is	long gone

A dead key plus buying the real one costs more than doing it right.





Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-home tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will make it right -- or refund it. No awkwardness, no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



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 comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech