BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

VPNs

What they are, what they really do, and whether you need one — explained in plain English, one step at a time

An honest, plain-English guide to consumer VPNs

No hype, no fear — just the straight story

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

Covers consumer VPNs & online privacy · facts current November 2026

What's Inside

This is your VPN manual, and it's an honest one. Read it in any order and at your own pace. A VPN is one of the most heavily advertised products online, and much of that advertising overstates what it does. This book explains plainly what a VPN really is, the handful of times it genuinely helps, the times it doesn't, and how to choose and use one without being scared or oversold.

Part 1 — The Honest Truth About VPNs

1 A Note from Bill
2 What a VPN Actually Is
3 The Advertising vs. the Reality
4 The Honest One-Sentence Answer

Part 2 — What a VPN Really Does & Doesn't

5 What a VPN Hides
6 The Padlock Already Protects You
7 What a VPN Does NOT Do

Part 3 — When a VPN Actually Helps

8 On Public Wi-Fi
9 Watching Shows from Elsewhere
10 Privacy from Your Internet Provider
11 Do You Actually Need One? A Checklist

Part 4 — What Actually Keeps You Safe

12 The Protections That Really Matter
13 The Scams a VPN Won't Stop
14 A Sensible Security Plan

Part 5 — If You Decide to Get One

15 Why Free VPNs Are Dangerous
16 Choosing a Reputable VPN
17 Setting Up & Using a VPN
18 Avoiding VPN Scams & Traps

Part 6 — Your Honest Summary

19 The Whole Truth on One Page
20 A Plain-English Glossary
21 Where to Learn More & When to Call Bill

PART 1

The Honest Truth About VPNs

What this book is, what a VPN actually is in plain words, the gap between the advertising and the reality, and the honest one-sentence answer to "do I need one?"

CHAPTER 1

A Note from Bill

Hello, and welcome. If you've seen the ads — on television, before a YouTube video, in your email — warning darkly that you *need* a **VPN** to stay safe online, and you've wondered whether that's true, this book is for **you**. And I'm going to give you something those ads never do: an honest answer.

I'm Bill. Helping folks feel at home — and safe — with their technology is what I do every day. I've no VPN to sell you and no reason to scare you. I wrote this book the way I'd talk it through at your kitchen table: plainly, honestly, with no jargon and no sales pitch.

Why this book is different

Here's the uncomfortable truth about most information you'll find on VPNs: a great deal of it is written by the VPN companies themselves, or by websites paid to recommend them. So it tends to overstate what a VPN does and stir up fear to sell you one. This book owes nothing to anyone. I'll tell you honestly what a VPN *does*, the handful of times it genuinely helps, the many times it doesn't, and how to decide for yourself — without hype and without fear.

WHAT THIS DOES FOR YOU

What you'll walk away with

A clear, honest understanding of what a VPN really is and does, so you can see through the advertising. The ability to decide, with open eyes, whether you actually need one. And if you do want one, how to choose and use it sensibly — and how to avoid the ones that would do you more harm than good. Knowledge, not fear.

The spirit of this book

I'm not here to talk you into a VPN or out of one. For some people, in some situations, a VPN is genuinely useful. For many others, it's an unnecessary expense that protects against dangers they don't actually face. My job is to give you the honest facts so *you* can decide. And if you ever want to talk it through, you're never on your own — call me at **(330) 200-8042**.

— Bill

CHAPTER 2

What a VPN Actually Is

Let's start by cutting through the mystery. The letters **VPN** stand for "Virtual Private Network," which tells you nothing useful. So forget the name, and here's what it actually is, in plain English.

A private tunnel for your internet

A **VPN** is a service that creates a kind of private, protected tunnel for your internet connection. Normally, when you visit a website, your internet travels fairly directly from your device to that website. With a VPN switched on, your internet first travels through the VPN company's computer (a "server") — inside a scrambled, private tunnel — and *then* goes out to the website. Two things result from this detour, and they're the whole point of a VPN:

- **Your internet is scrambled** (encrypted) between your device and the VPN company, so anyone snooping on your connection in between sees only gibberish.
- **Websites see the VPN company's location, not yours** — so a website thinks you're wherever the VPN server is, rather than at your home.

That's genuinely all it does

I want to be very clear, because the ads muddy this: those two things — scrambling your connection to the VPN, and hiding your location from websites — are essentially the whole of what a VPN does. It is a narrow, specific tool. It is *not* a magic shield that makes you safe from everything online, however much the advertising implies otherwise. Keep those two real functions in mind, and you'll see through most of the hype.

GOOD TO KNOW

A VPN is a tool, not a force field

The single most useful thing to understand about a VPN is that it's a *narrow tool* with two specific jobs — not a general-purpose "make me safe online" force field. Nearly every misleading VPN ad works by blurring that distinction, hinting that a VPN protects you from scams, viruses, identity theft, and more. It doesn't. Hold onto "narrow tool, two jobs," and the truth stays clear.

WHAT THIS DOES FOR YOU

Understand it, and the fear falls away

Once you see plainly what a VPN is — a private tunnel that scrambles your connection and hides your location — the scary advertising loses its grip. You can judge honestly whether those two specific things are worth paying for in *your* life, rather than buying out of a vague, manufactured fear. Clarity is the first gift of this book.

CHAPTER 3

The Advertising vs. the Reality

VPNs are among the most heavily advertised products on the internet, and the advertising is often misleading. It's worth looking at the common claims side by side with the reality, so you can recognize the sales tricks when you see them.

Common claims, honest answers

The ad says…	The honest truth
"Hackers can steal your data — get a VPN!"	On today's internet, nearly every website already scrambles your connection on its own (the little padlock). A VPN adds another layer, but you're far less exposed than the ads suggest.
"Stay completely anonymous online!"	A VPN hides your location from websites, but you're still tracked through your accounts, cookies, and logins. It does NOT make you anonymous.
"Protect yourself from identity theft!"	A VPN does little against identity theft, which usually comes from scams, breaches, and stolen passwords — none of which a VPN stops.
"Banks and hackers can see everything!"	Scare tactics. Your bank's website is already encrypted; a VPN changes little there.

Why the ads work this way

VPN companies make money by selling subscriptions, so their advertising is designed to make you feel unsafe and then offer the VPN as the cure. Much of what you'll read "reviewing" VPNs is also paid for by the companies. None of this means VPNs are useless — they have real uses, which we'll cover — but it does mean you should treat the advertising with healthy skepticism, the way you would any product that sells itself through fear.

HEADS UP

Fear is the salesman — don't buy from fear

Whenever a product is sold by frightening you — "you're not safe without this!" — that's your cue to slow down and look at the facts, not speed up and buy. VPN ads lean heavily on fear precisely because the honest, unexciting truth ("a narrow tool useful in a few situations") doesn't sell as well. Decide based on what a VPN really does for *your* life, not on the worry the ad stirred up.

WHAT THIS DOES FOR YOU

See through the sales pitch

Knowing how VPN advertising works — selling through fear, overstating the benefits — means you can watch those ads with a clear head, neither frightened nor fooled. You judge the product on its real merits, which is exactly how to make a sensible decision about any purchase. The ads lose their power the moment you see how they work.

CHAPTER 4

The Honest One-Sentence Answer

You probably came to this book with one real question: "Do I actually need a VPN?" Let me give you the honest answer upfront, in a sentence, and then the rest of the book explains it.

The short answer

For most ordinary people, doing ordinary things on their home internet, a VPN is not necessary — but there are a few specific situations where it's genuinely useful, and it's worth knowing which apply to you.

That's it. Not "everyone must have one" (the ads' line), and not "VPNs are useless" (the cynics' line), but the honest middle: a narrow tool, unnecessary for most everyday use, genuinely handy in a handful of specific cases. The whole point of the rest of this book is to help you work out whether *your* life includes those cases.

The two questions that decide it

By the end of this book, you'll be able to answer two simple questions, and together they decide whether a VPN is worth it for you:

1. **Do I regularly use the internet on Wi-Fi I don't control** — coffee shops, hotels, airports? (A VPN is most useful here.)
2. **Do I want to watch shows or reach websites that are blocked in my area**, or keep my internet activity private from my internet provider? (A VPN can help with these.)

If you answered a clear "no" to both, you very likely don't need a VPN, and can set the whole worry down. If you answered "yes" to either, read on — one may be worth having for you.

WHAT THIS DOES FOR YOU

A clear answer, free of fear

Having an honest framework — a narrow tool, unnecessary for most, useful in a few specific cases, decided by two simple questions — means you can settle the VPN question for yourself calmly and sensibly. No more nagging worry from the ads, no more uncertainty: just a clear-eyed decision based on your actual life. That's worth more than any VPN.

PART 2

What a VPN Really Does & Doesn't

A plain look at what a VPN hides and what it doesn't, why the padlock on websites already protects you, and where the real limits are.

CHAPTER 5

What a VPN Hides

Let's be precise about the two genuine things a VPN does for you, because understanding them clearly is how you judge whether they matter in your life.

1. It scrambles your connection to the VPN

Between your device and the VPN company, your internet traffic is **encrypted** — scrambled so that anyone who manages to snoop on your connection along the way sees only meaningless gibberish. This matters most on networks you don't control, like public Wi-Fi, where in theory someone nearby might try to peek at your traffic. On your own home internet, this is far less of a concern.

2. It hides your location (your "IP address") from websites

Every internet connection has an **IP address** — a sort of return address that reveals roughly where you are (your town, your internet company). With a VPN on, websites see the *VPN server's* address instead of yours, so they think you're wherever the server is — another city, or another country. This is what lets a VPN make it look like you're somewhere you're not, which has a few uses we'll come to.

And that's the honest list

Those two things — scrambling your connection to the VPN, and hiding your location from websites — are the real, genuine benefits of a VPN. Everything a VPN usefully does flows from these two. If neither of them solves a problem you actually have, a VPN has little to offer you, whatever the ads say.

> **GOOD TO KNOW**
>
> **Two real jobs — worth remembering**
>
> Scramble the connection, hide the location. Those are the two things a VPN does. Write them on a card if it helps. Every honest use of a VPN comes down to one of those two, and every misleading ad works by hinting it does far more. Keep the two real jobs firmly in mind, and you'll never be fooled about what a VPN can and can't do for you.

WHAT THIS DOES FOR YOU

Know exactly what you'd be buying

Understanding the two real functions of a VPN means that if you do decide to get one, you know exactly what you're paying for — and if you decide not to, you know exactly what you're passing up. No vague promises, no hidden magic: just two specific, understandable benefits you can weigh against your actual needs.

CHAPTER 6

The Padlock Already Protects You

Here's a crucial fact the VPN ads never mention, and it undercuts much of their fear: on today's internet, your connection to nearly every website is *already* scrambled and protected, all on its own, with no VPN needed. Understanding this is key to seeing why most people don't need a VPN for everyday browsing.

That little padlock does a lot

When you visit a website, look at the top of your browser for a small **padlock** symbol beside the address. That padlock means your connection to that website is **encrypted** — scrambled — so that your passwords, card numbers, and everything you send are protected from snooping, automatically. These days, the vast majority of websites — certainly every bank, shop, and email service — use this padlock protection as standard. You've been protected all along, without ever installing a thing.

What this means for the "hackers on Wi-Fi" scare

The classic VPN ad warns that on public Wi-Fi, "hackers can steal your passwords and credit cards." Years ago, before the padlock became universal, there was something to this. Today, because your connection to each website is already scrambled by that padlock, a snoop on the Wi-Fi can't read your passwords or card numbers even without a VPN. The danger the ads describe has largely been solved already, by the padlock, for free.

TIP

Look for the padlock before you type anything sensitive

Whether or not you ever use a VPN, build this habit: before typing a password or card number into any website, glance for the **padlock** beside the address, and make sure the website is really the one you meant (your real bank, not a look-alike). That padlock is your everyday protection, working automatically. A VPN can add a layer on top, but the padlock is doing the heavy lifting already.

WHAT THIS DOES FOR YOU

You're more protected than the ads admit

Knowing that the padlock already scrambles your connection to nearly every website — automatically, for free — takes much of the fear out of everyday browsing, and much of the wind out of the VPN ads' sails. For most ordinary online tasks, you're already well protected. A VPN adds a layer; it isn't the only thing standing between you and disaster, whatever the ad implied.

CHAPTER 7

What a VPN Does NOT Do

Just as important as knowing what a VPN does is knowing what it *doesn't* — because the ads imply it does far more, and believing that could give you a false sense of security about the dangers that actually matter. Here's the honest list of what a VPN will **not** protect you from.

A VPN does NOT:

- **Protect you from scams.** If a crook tricks you into giving up a password or sending money, a VPN does nothing — the danger was the trick, not the connection.
- **Protect you from viruses or bad software.** If you download something harmful, a VPN doesn't stop it.
- **Make you anonymous.** You're still tracked through your accounts, cookies, and logins. Log into Google or Facebook, and they know it's you, VPN or not.
- **Protect the information you type and hand over.** Fill in a form, post on social media, give a site your details — that's exposed regardless of a VPN.
- **Stop your passwords leaking in a company breach.** That happens on the company's end, far beyond your VPN.
- **Keep you safe from a fake website** you were tricked into visiting.

Why this matters

The real dangers most people face online — scams, tricked passwords, breaches, harmful downloads — a VPN does essentially nothing about. So if you bought a VPN believing it made you "safe online," you might let your guard down on the things that actually threaten you. The honest truth is that the habits in the next chapter protect you far more than any VPN ever could.

HEADS UP

A VPN is not a safety blanket — don't let it lull you

The real risk of believing the VPN hype isn't the money; it's the false comfort. If you think a VPN has made you "safe online," you may click a scam link or skip strong passwords, thinking you're protected — when a VPN does nothing against those real dangers. Whether or not you use a VPN, keep your guard up against scams and keep your passwords strong. Those are what truly protect you.

WHAT THIS DOES FOR YOU

No false security

Knowing exactly what a VPN won't do means you never rely on it for protection it can't give — and you keep your attention on the habits that genuinely keep you safe. That honest clarity is worth more than any product: it keeps you alert to the real dangers instead of lulled by a false sense of safety.

PART 3

When a VPN Actually Helps

The genuine, honest situations where a VPN earns its keep — public Wi-Fi, watching shows from elsewhere, and privacy from your internet provider — and a checklist to decide.

CHAPTER 8

On Public Wi-Fi

This is the most genuine everyday use of a VPN, so let's look at it honestly. When you use the internet on Wi-Fi you don't control — a coffee shop, a hotel, an airport, a library — a VPN adds a layer of protection that some people find worth having.

The honest picture

On public Wi-Fi, you're sharing a network with strangers, and in theory someone could try to snoop on the traffic. Now, as we learned, the padlock already scrambles your connection to each website, so your passwords and card numbers are protected even without a VPN. But a VPN scrambles *everything* — even the bits the padlock doesn't — and hides which websites you're visiting from anyone watching the network. For some, that extra layer on untrusted Wi-Fi brings genuine peace of mind.

Is it worth it for you?

Ask yourself honestly: do you *regularly* use the internet on public Wi-Fi for anything sensitive — checking your bank, say — at cafes, hotels, or airports? If you travel often and bank or shop on hotel Wi-Fi, a VPN is a reasonable, modest protection worth considering. If you almost always use your own home internet, this benefit barely applies to you, and a VPN would mostly sit unused.

TIP

The simplest public-Wi-Fi protection costs nothing

Here's a free alternative worth knowing: on your phone, you can often skip public Wi-Fi entirely and use your phone's own **cellular data** for sensitive things like banking — which isn't shared with strangers the way public Wi-Fi is. And on a laptop, you can create a personal "hotspot" from your phone. For occasional sensitive tasks away from home, that's often simpler and cheaper than a VPN.

WHAT THIS DOES FOR YOU

A reasonable comfort for frequent travelers

If you're often on hotel and airport Wi-Fi doing things that matter, a VPN is a sensible, modest layer of protection and peace of mind — one of its few genuinely useful everyday roles. If you're a homebody on your own trusted internet, you can note this benefit and move on, knowing it doesn't much apply to you.

CHAPTER 9

Watching Shows from Elsewhere

Another genuine use of a VPN — and an honest one — is making it look like you're in a different place, which can let you watch shows or reach websites that are blocked where you are. Let's look at this plainly, including its real limits.

How it works

Because a VPN hides your real location and makes websites think you're wherever the VPN server is, you can appear to be in another city or country. People use this to watch a streaming service's shows that are only available in another region, to catch a sporting event blacked out locally, or to reach a website that's blocked where they are. Pick a VPN server in, say, Britain, and some services will show you what a viewer in Britain would see.

The honest limits

- **It's unreliable.** Streaming services actively try to block VPNs, so it often doesn't work, or stops working after a while. You may pay for a VPN and find it won't do the one thing you wanted.
- **It may break the service's rules.** Using a VPN to watch region-locked content often goes against the streaming service's terms — rarely enforced against individuals, but worth knowing.
- **It can slow things down.** Routing your video through a distant server can cause buffering.

GOOD TO KNOW

A real use, but a fickle one

Watching region-locked shows is a genuine thing VPNs *can* do — but it's the ficklest of their uses, because the streaming services are in a constant tug-of-war to block them. So if this is your main reason for wanting a VPN, go in with modest expectations: it may work today and not next month. Don't pay for a long VPN subscription counting on it, when it might stop working at any time.

WHAT THIS DOES FOR YOU

Honest expectations, no disappointment

Knowing that a VPN *can* unlock shows from elsewhere, but unreliably, means you can try it for that purpose with your eyes open — pleased if it works, unsurprised if it doesn't. That honest expectation saves you from the frustration of paying for a VPN expecting magic and getting a blocked screen. A real use, with real limits, understood upfront.

CHAPTER 10

Privacy from Your Internet Provider

A third honest use of a VPN is keeping your internet activity private from your **internet provider** — the company you pay for your home internet. Whether this matters to you is a personal judgment, so let's look at it fairly.

What your provider can see

Your internet provider (your cable or phone company) can see which websites you connect to, even if they can't read the scrambled contents (thanks to the padlock). Some providers keep records of this, and in some places may use or sell information about customers' browsing habits. With a VPN on, your provider sees only that you're connected to the VPN — not which sites you then visit through it. Your browsing becomes private from them.

Does this matter to you?

This is genuinely a matter of personal preference. Some people simply dislike the idea of their internet company being able to see (and perhaps record or sell) which websites they visit, and value the privacy a VPN gives from that. Others aren't troubled by it. Neither view is wrong. If the thought of your provider watching your browsing bothers you, this is a real reason some people choose a VPN; if it doesn't, you can set it aside.

GOOD TO KNOW

You're trading one watcher for another

An honest wrinkle to weigh: a VPN hides your browsing from your internet provider — but the *VPN company* can now see it instead. You're moving your trust from your cable company to the VPN company. A good, reputable VPN promises not to keep records of your activity, but you're trusting that promise. So this benefit is really "I'd rather trust the VPN company than my internet provider" — a reasonable choice, but a trade, not a disappearance.

WHAT THIS DOES FOR YOU

A clear-eyed personal choice

Understanding exactly what a VPN hides from your internet provider — and that you're trusting the VPN company in exchange — lets you decide this on your own terms, based on what you value. For some, that privacy is genuinely worth it; for others, it isn't a concern. Either way, you're choosing with the full, honest picture.

CHAPTER 11

Do You Actually Need One? A Checklist

Let's pull it all together into a simple, honest checklist so you can decide for yourself. Go through these, and your answer will become clear.

A VPN may be worth it for you if…

- You **often use public Wi-Fi** (hotels, airports, cafes) for sensitive things like banking.
- You **travel a lot** and connect to untrusted networks regularly.
- You want to **watch shows or reach sites** available only in other regions (accepting it may be unreliable).
- You feel **strongly about privacy** from your internet provider.
- You need it for **work** (many jobs require a VPN to reach company systems — if so, your employer provides it and tells you how).

You very likely DON'T need one if…

- You **mostly use your own home internet**, which you trust.
- You do **ordinary things** — email, browsing, shopping, video calls — and the padlock already protects them.
- You **don't travel much** or rarely use public Wi-Fi for anything sensitive.
- You bought the idea from an **ad** and can't name a specific problem it would solve for you.

TIP

If you can't name the problem, you don't need the product

Here's a simple test for a VPN, or any product sold through fear: can you name a specific, real problem in *your* life that it would solve? "I bank on hotel Wi-Fi twice a month" is a real problem a VPN helps with. "The ad said I need one" is not. If you can't point to a concrete situation where you'd actually use it, that's your answer — save your money with a clear conscience.

WHAT THIS DOES FOR YOU

A confident decision, either way

Whether the checklist points you toward a VPN or away from one, you now decide from honest facts rather than advertising fear. If you need one, you know why and what for; if you don't, you can ignore the ads for good. That settled confidence — knowing you've chosen sensibly for your own life — is exactly what this book set out to give you.

PART 4

What Actually Keeps You Safe

Since a VPN won't protect you from the real dangers, here's what truly does — the handful of habits worth far more than any VPN subscription.

CHAPTER 12

The Protections That Really Matter

If you take only one thing from this book, let it be this chapter. The things that genuinely keep you safe online have almost nothing to do with a VPN — and they're mostly free. Here's where your attention (and any money) is far better spent.

The real safety essentials

Protection	Why it matters far more than a VPN
Strong, different passwords	A different, strong password on each important account, remembered by a password manager. This defeats the most common way people actually get hurt.
Two-factor authentication	An extra code or tap on top of your password for important accounts. The single best protection against stolen passwords.
Keeping things updated	Letting your phone, computer, and apps update themselves, which closes security holes crooks exploit.
Caution against scams	Not clicking suspicious links, not giving passwords or codes to callers, not being rushed. Most real harm comes from being tricked, not hacked.
Backups	A safe copy of your photos and files, so a lost or broken device isn't a disaster.

Why these beat a VPN

Look at that list against what a VPN does, and the truth is plain: these habits protect you from the dangers people *actually* face — scams, stolen passwords, breaches, harmful downloads — while a VPN protects against a narrow, less common threat. If you've not yet set up strong passwords and two-factor, doing so protects you far more than any VPN subscription ever would. Spend your effort here first.

TIP

Do these before you ever think about a VPN

If you're worried about online safety and wondering whether to buy a VPN, here's my honest advice: first make sure you have strong, unique passwords (ideally in a password manager) and two-factor turned on for your email and bank. Those two things, both free, protect you more than a VPN ever could. Get them in place, and you may find your safety worry is answered without spending a penny on a VPN. (We have whole manuals on passwords, too.)

WHAT THIS DOES FOR YOU

Real safety, mostly free

The genuine protections — good passwords, two-factor, updates, scam awareness, backups — cost little or nothing and defend against the dangers you actually face. Putting these in place gives you real, solid safety, the kind no VPN can match. That's where peace of mind truly comes from, and it's within everyone's reach.

CHAPTER 13

The Scams a VPN Won't Stop

Because scams are the single biggest online danger to ordinary people — and a VPN does nothing against them — it's worth a clear reminder of what they look like, so you're protected where it counts. A VPN running in the background would not have stopped a single one of these.

The scams that actually hurt people

- **The scary pop-up or call** — "Your computer is infected, call this number!" A fake, designed to get money or access. A VPN does nothing against it.
- **The urgent "account problem" message** — an email or text pushing you to click a link and "verify" your bank or account. The trick works whether or not you have a VPN.
- **The grandchild in trouble** — a call claiming a loved one urgently needs money. No VPN helps here.
- **The gift-card demand** — anyone asking to be paid in gift cards is a scammer. A VPN is irrelevant.
- **The "tech support" who wants remote access** — a stranger talking you into letting them control your computer. A VPN offers no protection.

What protects you from these

The protection against every one of these is the same, and it's not a product: it's **awareness and a healthy pause.** When something rushes you, frightens you, or asks for money, a password, or a code — stop, and don't act. That simple habit defeats the scams that a VPN is powerless against, which happen to be the ones that actually cost people dearly.

SCAM ALERT

When in doubt, stop and call me

If a call, email, text, or pop-up ever makes you uneasy — about money, a password, your accounts, anything — **stop and call me before you do a single thing**, at **(330) 200-8042**. I'll never charge you, and never think less of you, for a "is this a scam?" question. These scams, not snoopers on Wi-Fi, are what truly threaten people — and a free call to a friend protects you far better than any VPN.

WHAT THIS DOES FOR YOU

Guarding against the real threat

Keeping your guard up against scams — the dangers that actually cost ordinary people their money and peace of mind — protects you where a VPN never could. Knowing the scams' playbook, and that a free "is this real?" call is always available, is worth more than any subscription. That's real security, aimed at the real danger.

CHAPTER 14

A Sensible Security Plan

Let's put the honest picture together into a simple, sensible plan — so you know exactly where a VPN fits (if at all) among the things that actually keep you safe. Think of it as priorities, in order.

Your safety priorities, in order

1. **Strong, unique passwords** on your important accounts (a password manager makes this easy). — Free, essential.
2. **Two-factor authentication** on your email and bank. — Free, essential.
3. **Keep everything updated** — phone, computer, apps. — Free, automatic.
4. **Stay alert to scams** — pause when rushed; verify; never share codes. — Free, vital.
5. **Back up your photos and files.** — Cheap or free, invaluable.
6. **A VPN** — only if the checklist in Part 3 showed a real use for you (public Wi-Fi, region-locked shows, provider privacy). — Optional, situational.

Where a VPN sits

Notice where the VPN lands: *last*, and *optional*. That's its honest place in a sensible security plan — a useful extra for specific situations, not a foundation. Get the first five in place, and you're genuinely well protected. Add a VPN on top only if you have a real use for it. Done in this order, your money and effort go where they do the most good.

TIP

Build from the foundation up

Don't let a VPN be the *first* thing you do for online safety — that's building the roof before the walls. Start with the free essentials (passwords, two-factor, updates, scam-awareness, backups), which protect you from the real dangers. Then, and only then, consider a VPN if your life includes one of its genuine uses. Foundation first, extras after.

WHAT THIS DOES FOR YOU

Real protection, sensibly prioritized

A sensible plan — the free essentials first, a VPN only if you truly need it — gives you genuine, well-rounded safety without wasted money or false comfort. You protect against the dangers that matter most, in the order that matters most, and you add a VPN only where it earns its place. That's security done honestly and well.

PART 5

If You Decide to Get One

For those who have a genuine use: why free VPNs are dangerous, what to look for in a paid one, how to set it up and use it, and how to avoid the deals that are traps.

CHAPTER 15

Why Free VPNs Are Dangerous

If the checklist showed you have a real use for a VPN, your first instinct might be to find a **free** one. Please don't — this is the one place I'll be firm with you. A free VPN is often worse than no VPN at all, and here's the honest reason why.

If it's free, you're the product

Running a VPN — all those servers handling everyone's internet — costs the company real money. So a free VPN has to make its money somehow, and far too often, that "somehow" is *you*: by watching what you do online and selling that information, by injecting ads, or worse. The whole point of a VPN is privacy, and a free one frequently does the exact opposite — spying on you and selling you out. Studies have caught free VPNs tracking users, selling browsing data, and even carrying harmful software.

The honest rule

Never use a free VPN. The small saving isn't worth the risk of handing your entire internet activity to a company whose business is selling it. If a VPN is worth having for your situation, it's worth paying a modest amount for a reputable one; and if it's not worth a few dollars a month to you, then it's not worth using a dangerous free one — you simply don't need a VPN. There's no good middle ground here.

HEADS UP

A free VPN can be worse than none at all

This is the one firm warning in this whole book: **avoid free VPNs entirely.** Because a VPN sees all your internet traffic, trusting a shady free one with it is genuinely dangerous — you could be handing your browsing straight to people who'll misuse it. If you have a real need for a VPN, pay a little for a reputable one; if you won't pay, you don't need one badly enough to risk a free one. No exceptions.

WHAT THIS DOES FOR YOU

The right choice is clear

Knowing the truth about free VPNs makes the decision simple and safe: a reputable paid one if you have a genuine use, and nothing at all otherwise — never a risky free one. That clarity protects you from a trap that catches many well-meaning people who thought they were doing something safe. When it comes to VPNs, free is a false bargain.

CHAPTER 16

Choosing a Reputable VPN

If you've decided a VPN is worth it for your situation, let's choose a good one sensibly. I won't name specific brands — they change, and I don't want to steer you toward a paid recommendation — but here's what to look for, and how to cut through the misleading "best VPN" lists.

What to look for

- **A well-established, reputable company** with a long track record — not a name you've never heard of.
- **A clear "no-logs" promise**, ideally one that's been independently checked — meaning they promise not to keep records of your activity.
- **A reasonable, honest price** — a few dollars a month. Be wary of "lifetime" deals and prices that seem too good to be true.
- **Easy-to-use apps** for your devices, so you can turn it on and off simply.
- **A money-back trial**, so you can test that it actually does what you need (like unblocking a show) before committing.

Ignoring the misleading "reviews"

Be very skeptical of "Top 10 Best VPNs" websites — many are paid to rank whichever company pays most, not whichever is best. They're advertising dressed up as advice. Instead, favor long-established names with good reputations, read independent (non-affiliate) sources if you can find them, and don't be swayed by a flashy ranking. When in doubt, ask someone you trust — including me.

FROM BILL

Happy to help you pick a sensible one

If you've decided a VPN would genuinely help you — say you travel and bank on hotel Wi-Fi — I'm glad to help you choose a reputable one at a fair price, and steer you clear of the dodgy free ones and the misleading "best VPN" traps. No sales pitch, no pressure — just honest help picking a sensible tool for your real need. **(330) 200-8042**.

WHAT THIS DOES FOR YOU

A good tool, chosen wisely

Knowing what to look for — a reputable company, a checked no-logs promise, an honest price, a trial — and how to ignore the paid "reviews" means that if you do get a VPN, you get a genuinely good one, not a trap. You pay a fair price for a tool that does what you need, chosen with clear eyes rather than swayed by advertising.

CHAPTER 17

Setting Up & Using a VPN

Using a VPN, once you've chosen one, is refreshingly simple — it's mostly an on/off switch. Let's walk through what to expect, so there are no surprises.

Getting started

1. **Sign up** on the VPN company's website and pay for your subscription.
2. **Install their app** on your device — from the official app store (iPhone/Android) or the company's own website (computer). Only ever from these official sources.
3. **Sign in** to the app with your new account.
4. **Turn it on** — usually a single big button that says "Connect." That's it: the VPN is now protecting your connection.

Everyday use

- **To turn it on:** open the app and tap **Connect** (or it can connect automatically).
- **To appear in another place** (for shows): choose a server location in the app before connecting.
- **To turn it off:** tap **Disconnect**. You don't have to leave it on all the time — many people turn it on only for public Wi-Fi or a specific task.
- **A small sign** (often a little key or "VPN" symbol) usually shows at the top of your screen when it's on.

TIP

You don't have to leave it on all the time

A common misunderstanding: you needn't run your VPN constantly. Many people turn it on only when they actually need it — on public Wi-Fi, or to watch a particular show — and off the rest of the time, since leaving it on can slow your internet a little. Use it *when it helps*, and switch it off otherwise. It's a tool to pick up and put down, not a thing that must run forever.

WHAT THIS DOES FOR YOU

Simple to use, when you want it

A VPN comes down to a single on/off button, used when it helps and ignored otherwise. Once it's set up, there's nothing complicated about it — connect for the hotel Wi-Fi or the show you want, disconnect after. Knowing it's that simple takes away any worry about using one, if you've decided it's worth having.

CHAPTER 18

Avoiding VPN Scams & Traps

Ironically for a product sold as protection, the VPN world has its own scams and traps. Since you're reading this to be sensible, let's cover the ones to watch for, so you don't get caught.

The traps to avoid

- **"Lifetime" VPN deals.** A VPN costs the company money forever, so a one-time "lifetime" price often means the company plans to cut corners, sell your data, or vanish. Be very wary.
- **Free VPNs** (covered already) — the biggest trap of all.
- **"Your device is at risk — install this VPN now!" pop-ups.** These are scams, not real warnings. Never install a VPN (or anything) from a pop-up.
- **Auto-renewing subscriptions** you forget about — note when yours renews, and cancel if you've stopped using it.
- **Unknown brands with amazing prices** — if it seems too cheap and too good, be suspicious.

The safe path

Stick to a reputable, established VPN company, sign up only on their genuine website, install their app only from the official app store or their site, pay a fair monthly or yearly price (not a "lifetime" one), and keep track of when it renews. Do that, and you sidestep the traps entirely. And if any VPN ad or pop-up pressures or frightens you into acting fast, that pressure itself is the warning sign.

SCAM ALERT

Never install a VPN from a pop-up or scary warning

A real VPN is something *you* seek out and sign up for deliberately. If a pop-up, ad, or "warning" ever urges you to install a VPN right now to "protect" or "fix" your device, it's a scam — close it, and don't install a thing. The same goes for any security product pushed on you by a pop-up. When in doubt, don't, and call me — that's exactly the kind of thing I'm glad to check for you, free.

WHAT THIS DOES FOR YOU

A VPN that helps, not one that harms

Knowing the VPN world's own traps — lifetime deals, free ones, pop-up "warnings," forgotten renewals — means that if you get a VPN, you get a genuine, reputable one that actually helps, and you avoid the many that would take your money or your data. You end up with the real thing, chosen and used wisely, free of the traps that catch the unwary.

PART 6

Your Honest Summary

The whole truth on one page, a plain-English glossary, where to learn more, and my standing offer to help you decide.

CHAPTER 19

The Whole Truth on One Page

Here's everything in this book, boiled down to a page you can keep. Read it whenever a VPN ad tries to worry you, and you'll remember the honest truth.

What a VPN is and does

- A VPN is a **narrow tool** with two real jobs: it **scrambles your connection** to the VPN company, and **hides your location** from websites.
- That's *all* it does. It is not a magic shield against everything online.

When it helps — and when it doesn't

A VPN CAN help with…	A VPN does NOT help with…
Public Wi-Fi (hotels, cafes)	Scams and tricks
Watching region-locked shows (unreliably)	Viruses and bad downloads
Privacy from your internet provider	Stolen passwords & breaches
Work access (your employer sets it up)	Making you anonymous
	Anything you type or hand over

The honest bottom line

- **Most people doing ordinary things on home internet don't need a VPN.**
- **The padlock already protects your connection to websites, for free.**
- **Strong passwords, two-factor, updates, and scam-awareness protect you far more than any VPN** — do these first.
- **If you do get one: never a free VPN; choose a reputable paid one; avoid "lifetime" deals and pop-ups.**
- **When in doubt, ask — and never buy out of fear.**

TIP

The one question that settles it

If an ad has you wondering whether you need a VPN, ask yourself: *can I name a specific situation in my own life where I'd actually use it?* If yes (regular hotel Wi-Fi banking, say), consider a reputable paid one. If no, you don't need it — set the worry down for good, and spend your effort on the free protections that actually matter.

CHAPTER 20

A Plain-English Glossary

If a term ever trips you up, look it up here.

Term	In plain English
VPN	A service that makes a private, scrambled tunnel for your internet and hides your location. Stands for "Virtual Private Network."
Encryption	Scrambling information so only the right party can read it — meaningless gibberish to a snooper.
IP address	A sort of return address for your internet connection that reveals roughly where you are.
Server	A powerful computer; a VPN routes your traffic through the company's servers.
The padlock (HTTPS)	The symbol by a website's address showing your connection to it is already scrambled — your everyday protection.
Public Wi-Fi	Internet at a cafe, hotel, or airport that you don't control and share with strangers.
Region-locked	Content (like a show) available only in certain countries or areas.
No-logs	A VPN company's promise not to keep records of your activity.
Free VPN	A VPN with no fee — often dangerous, as it may sell your data. Avoid.
Internet provider	The company you pay for home internet (your cable or phone company).
Two-factor authentication	An extra code or tap on top of your password — a real protection, unlike a VPN, against stolen passwords.
Cellular data	Internet over the phone network, not shared like public Wi-Fi — often a free alternative to a VPN away from home.

CHAPTER 21

Where to Learn More & When to Call Bill

You've reached the end — and you now understand VPNs better than most people who buy them. Here's where to turn for more, and a few parting words from me.

Good places to learn more

- **Independent (non-affiliate) tech sites** — look for reviews that aren't paid placements. Consumer-advocacy and non-profit sources are often the most honest.
- **GCFGlobal.org** — free, patient lessons on internet safety for beginners, with no products to sell.
- **Our other manuals** — "Passwords & Password Managers" covers the protections that actually keep you safe, far more than a VPN.
- **And me, anytime** — when you'd rather get an honest, no-sales-pitch answer from a real person.

A few parting words

Here's the truth to carry away: **a VPN is a narrow tool, useful for a few people in a few situations, and oversold to everyone else by fear.** You don't have to be afraid of the ads anymore, because now you know what a VPN really does — and what it doesn't. That knowledge is worth more than the product.

If your life includes a genuine use for a VPN, get a reputable paid one and use it sensibly. If it doesn't, set the whole worry down with a clear conscience, and put your effort into the free protections that genuinely keep you safe. Either way, you're deciding from honest facts, which is exactly as it should be.

And remember the bigger picture: the dangers that actually threaten ordinary people are scams, not snoopers. Keep your guard up there, and when something feels off, call me before you act.

How I can help

I'm Bill, and helping folks feel at home — and genuinely safe — with their technology is what I've done for more than 30 years. I serve **Portage County, Ohio**, in plain English, with no products to sell and no fear to peddle — whether that's helping you decide if a VPN is worth it, picking a reputable one if so, or (more often) setting up the free protections that matter far more. There's never any rush, and you can book a visit any time at

billshometech.com/book.

FROM BILL

My standing offer

If you're wondering whether you need a VPN — or any product sold through fear — pick up the phone before you buy. I'll give you an honest answer for your situation, with no sales pitch, and help you spend your effort where it actually keeps you safe. That honest, friendly second opinion is exactly what I'm here for.

— Bill · Bill's Home Tech · (330) 200-8042 · BillsHomeTech.com/book