SAILING DIRECTIONS FOR SMALL BUSINESSES

Before you pay for a website

Anyone can now make a website in an afternoon with an AI tool, and plenty of people are selling the results as professional work. Here's what can go wrong, and how to tell the difference before you pay.

WHAT'S CHANGED
Why a site that works can still be unsafe

WHAT GOES WRONG
Security, the law, and who owns what

BEFORE YOU HIRE
Questions to ask, and the answers to listen for

AT THE BACK
A checklist to take to any meeting

Robert
Tideswell



BEFORE WE START

Hi, I'm Rob. This one's a friendly warning.

Over the last year or so a new kind of web developer has turned up. They're quick and cheap, and the sites look great in the demo. Some of them have no idea what's underneath.

I build websites, tills and software for small businesses in Lincolnshire. AI coding tools are used right across my trade now, and used properly they're genuinely useful. The trouble is they've made it possible to sell a website without understanding a line of it, and when something goes wrong it's usually the business that pays for it, not the person who built it.

This isn't about putting you off hiring anyone, or off AI. It's the list of things I'd want a friend to check before handing over money, whoever they hire. Me included.

THE ONE QUESTION I'D ASK

"How are my customers' details kept safe?" A good developer can answer that in plain English in a minute or two. If you get a shrug, a wall of jargon or "the AI handles all that", keep looking.

How to use it: section 1 explains what's changed. Sections 2 to 4 cover what goes wrong, and sections 5 and 6 are what to ask and what to look out for. Section 7 is for anyone who already has a website and is now wondering. The checklist at the back fits on one page, so take it to the meeting.

01 WHAT'S CHANGED 3

02 THE SECURITY PROBLEMS YOU CAN'T SEE 4

03 THE LAW, AND WHO'S RESPONSIBLE 5

04 WHO OWNS IT 7

05 QUESTIONS TO ASK ANY DEVELOPER 8

06 RED FLAGS, AND GOOD SIGNS 9

07 ALREADY GOT A WEBSITE? 10

08 THE CHECKLIST 11

01 WHAT'S CHANGED

Making a website got easy. Checking it didn't.

In 2025 a new phrase caught on: "vibe coding". It means building software by describing what you want to an AI tool and accepting whatever it writes, without reading it. For a hobby project that's fine. For a website that takes bookings, payments or customers' details, it's a gamble.

The tools write code that runs and looks finished. Whether it's safe is a different question, and you can't tell by looking at the website. Neither can the person who made it, if they never read the code.

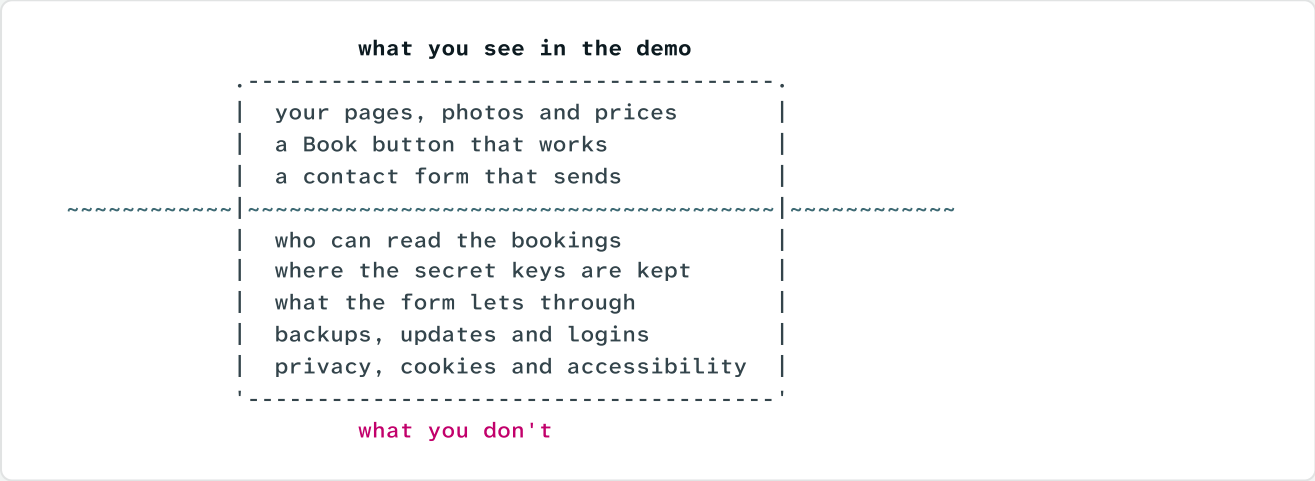


FIG. 1 · MOST OF A WEBSITE IS BELOW THE WATERLINE

What the research says

45%

More than 100 AI models were given coding tasks that could be done safely or unsafely. They picked the unsafe way 45% of the time.

VERACODE, GENAI CODE SECURITY REPORT, 2025

1 in 5

In 576,000 samples of AI-written code, about one in five add-ons it asked for didn't exist. Criminals now publish harmful add-ons under those made-up names.

USENIX SECURITY SYMPOSIUM, 2025

23.8m

Passwords and secret keys found in public code on GitHub in 2024, up a quarter on the year before.

GITGUARDIAN, STATE OF SECRETS SPRAWL, 2025

THE TOOL ISN'T THE ISSUE

Plenty of good developers use AI tools. They read and test everything it writes, and they can tell when it's wrong. The risk is someone who can't, selling the result as professional work.

02 THE SECURITY PROBLEMS YOU CAN'T SEE

Six problems that never show up in a demo

Each of these is common in websites built by someone who doesn't read the code, and each one costs real money when it goes wrong.

01 Secret keys left in the page

Websites talk to other services, like card payments, email and maps, using secret keys that work like passwords. AI tools often put them straight into the code that every visitor's browser downloads, where anyone can read them. **What it means for you:** strangers running up bills on your accounts, sending spam in your name, or reading your customers' orders.

02 Databases anyone can open

Many AI app builders keep bookings, orders and sign-ups in an online database with access rules. If nobody switches the rules on, anyone who knows where to look can read or change the lot. In 2025 a flaw of exactly this kind, rated critical, was found in sites made with one popular AI app builder. **What it means for you:** a data breach you may have to report.

03 Forms with no checks

A contact or booking form that doesn't check what's typed into it can be used to send spam through your website, or to slip harmful code into your pages. In the study on the last page, AI models failed to guard against that second one in 86% of cases. **What it means for you:** your emails landing in junk folders, your host suspending the site, or visitors attacked through it.

04 Logins and admin pages

An editor or admin page with a weak password, no limit on guesses and no two-step login is an open door. So is one left switched on "for testing". **What it means for you:** someone else changing your prices or putting their own content on your site.

05 Nobody looking after it

Websites are built from parts made by other people, and those parts get security fixes all the time. Someone has to apply them and check the backups actually work. With a site generated in an afternoon, often nobody does. **What it means for you:** a site that's safe the day it goes live and a bit less safe every month after.

06 Made-up add-ons

AI tools sometimes ask for add-ons that don't exist, and criminals publish harmful ones under those names. A developer who installs whatever the AI asks for can put one straight into your site. **What it means for you:** someone else's code running on your website.

ROCKS AHEAD: "IT WORKS" ISN'T A SECURITY CHECK

A site can look perfect and take bookings all day while leaking every one of them. The only way to know is for someone who understands the code to check it.

03 THE LAW, AND WHO'S RESPONSIBLE

If the website breaks the law, it's usually your problem

Under UK law, the business that collects customers' details and sells to them is responsible for how its website treats them. That's true whoever built it and whatever tools they used. AI tools aren't reliable on UK law, and they don't check their work against it.

This is a summary to point you in the right direction, not legal advice.

01 A privacy notice that's true

If the site collects any personal details at all (a contact form, bookings, a mailing list, visitor statistics), you need a privacy notice. It has to describe what your site actually does. A generic one produced in seconds often lists things your site doesn't do and misses things it does. Since June 2026 it should also tell people how to complain to you about how you've used their information.

02 The ICO fee

Most businesses that keep customers' details on a computer or phone have to pay the Information Commissioner's Office a yearly fee. For a business with up to 10 staff or a turnover up to £632,000 it's £52, or £47 by direct debit. Developers rarely mention it. The ICO's self-assessment at `ico.org.uk` takes a couple of minutes.

03 Cookies and tracking

The rules relaxed in February 2026 for simple visitor counting, but advertising and tracking cookies, like Facebook and Google ad pixels, still need a proper choice where saying no is as easy as saying yes. Fines went up at the same time, to as much as £17.5 million or 4% of turnover. Ask what the site loads, because embedded videos, maps and add-ons can set cookies of their own.

04 If customers' details leak

A data breach that puts people at risk has to be reported to the ICO within 72 hours of you finding out, and the people affected told if the risk is high. It's the business that reports it, not the developer.

05 Accessibility

Under the Equality Act 2010, businesses mustn't put disabled customers at a disadvantage, and that covers websites. Generated pages often have pale text, buttons a screen reader can't name and forms with no labels. The accepted standard to check against is WCAG 2.2.

06 Your business details

Every business website has to show your business name, a postal address and an email address, and your VAT number if you're registered. A limited company also needs its full registered name, company number, registered office and where it's registered, such as "Registered in England and Wales".

03 THE LAW, CONTINUED

07 Selling online

Before someone pays, you must tell them who you are, what they're getting, the total price including VAT and delivery, when it'll arrive and their right to cancel. For most goods that's 14 days, with sensible exceptions such as food and made-to-order items. Since April 2025, an advertised price must include any fees people can't avoid, like a compulsory booking fee.

08 Reviews and testimonials

AI tools often fill a new page with made-up testimonials as placeholders. If they go live, that's a fake review. Since April 2025 fake reviews are banned outright, and the Competition and Markets Authority can fine businesses directly.

09 Marketing emails

A "send me offers" box must be left unticked for people to tick themselves, and every marketing email needs an unsubscribe link that works. A pre-ticked box isn't consent.

10 Copyright

Photos, fonts, music and words all have owners. A generated site can include a font nobody has a licence for, or photos lifted from somewhere else, and photo agencies use software to find their pictures on small business websites. The bills can run to hundreds of pounds. AI-generated images can also look uncomfortably like someone else's work.

WHERE TO READ MORE

- Privacy notices, the ICO fee, cookies and breaches: `ico.org.uk`
- Selling online: `gov.uk/online-and-distance-selling-for-businesses`
- Company details on your website: `gov.uk/running-a-limited-company`
- Prices and reviews: the CMA's guidance on `gov.uk`
- Keeping a small business safe online: `ncsc.gov.uk`

04 WHO OWNS IT

Make sure you own what you're paying for

One of the most common website problems has nothing to do with hacking. It's a business that can't get into its own website, because everything is in somebody else's name.

WHAT	WHO SHOULD OWN IT	WHY
Your web address	You, in your own account	Lose it and you lose your Google ranking, your printed menus and often your email with it.
Hosting	You, or it's in writing that the site is yours	If the developer stops paying, the site goes offline.
The AI builder account	You	Many AI-built sites only run inside the builder's own platform. If the account isn't yours, neither is the site.
The files and code	You, with your own copy	So another developer can pick it up if you ever need one.
Your business email	You	It's usually tied to the web address.
Google Business Profile	You, as primary owner	Make your developer a Manager, never the owner.

Get these in writing before you pay

- Who owns the website and the web address once it's finished.
- What happens if the developer stops trading, or you part ways.
- What any monthly fee covers, and what it doesn't.
- How you get a full copy of your site and everything customers have sent through it.
- Who applies security updates, how often, and who checks the backups.
- A list of every account and login the site depends on.

ROCKS AHEAD: THE "FREE" WEBSITE

Some cheap or "free" deals keep the site, the web address or both in the seller's name. When you stop paying, they keep them. Read the small print, and ask outright who owns the domain.

05 QUESTIONS TO ASK ANY DEVELOPER

What to ask, and what to listen for

You don't need to understand the technical side to ask these. Listen for clear, specific answers. Anyone who knows their stuff will be happy to explain.

ASK	A GOOD ANSWER SOUNDS LIKE	WORRY IF YOU HEAR
How are my customers' details kept safe?	Where they're stored, who can get at them, and how that's been tested	"It's all secure" and nothing more
Who will own the web address, hosting and code?	"You will, in your own accounts. I'll help you set them up."	"We look after all that"
Where are passwords and secret keys kept?	On the server, never in the page, with two-step login on the admin	They don't understand the question
What about updates and backups?	Who does them, how often, and where the backups are kept	"It doesn't need any"
What do I need legally, and will the site have it?	A privacy notice written for your site, cookies handled, your business details, accessibility checked	"Just copy one from another site"
Can I see sites you've built that are live now?	Two or three working sites, and a past client you can ring	Only screenshots, or demos that no longer work
If you use AI tools, how do you check what they write?	They read and test it, and can explain any part of it	"I don't need to, it just works"
What happens if you stop trading?	Everything handed over, with a written list of every login	A long pause
Is that the whole price?	An itemised quote, with yearly costs like the domain, hosting and email spelled out	A low price now and "we'll see" later

IF THEY GET DEFENSIVE

A good developer is glad you asked, because it means you'll look after the site properly. If questions like these annoy someone, that tells you something too.

06 RED FLAGS, AND GOOD SIGNS

What to look out for

One red flag on its own isn't proof of anything. Two or three together usually mean it's worth walking away.

Red flags

- A full website with bookings or a shop promised in a day or two for very little money.
- They can tell you that something works, but not how.
- Everything goes in their name or their account.
- No privacy notice on their own site, or one that names a different company or country.
- Testimonials on their site that can't be traced to a real business.
- Placeholder text like "Lorem ipsum" or "Your Company Name" left on sites they've built.
- "Page one of Google, guaranteed."
- A price that only lasts if you sign today.

Good signs

- They ask about your business and your customers before they talk about design.
- They put the web address and hosting in your name without being asked.
- They can show you live sites and put you in touch with past clients.
- They tell you the yearly running costs up front.
- They bring up privacy, accessibility and backups before you do.
- They're happy to say what they don't do, and who they'd send you to.

TRY THIS ON THEIR OWN WEBSITE

A developer's own site is the one they had complete control over, so it's a fair sample. Open it on your phone and look for a privacy notice and an honest cookie message. Send a message through the contact form and see if you get a reply. Then put the address into `wave.webaim.org` for an accessibility check and `securityheaders.com` for a basic security check. Neither needs any technical knowledge to read.

BE WARY OF

Being rushed. A good developer is busy, but never too busy to answer your questions properly before you sign anything.

07 ALREADY GOT A WEBSITE?

Seven checks you can do yourself

None of these need technical knowledge. If one fails, it doesn't mean you've been hacked. It means it's worth asking some questions.

01 **Find out where your web address is registered, and log in.** If you can't, sort that out before anything else.

02 **Log in to the hosting or website builder account.** Check it's in your name, and that two-step login is on.

03 **Read your privacy notice.** Does it name your business, and describe what your site really collects?

04 **Send yourself a message through your own contact form.** Did it arrive, and not in junk?

05 **Put your address into `securityheaders.com` and `pagespeed.web.dev`.** A poor score is a reason to ask, not to panic.

06 **If you take card payments, check where the card details are typed.** They should go into the payment company's own page or box (Stripe, Square, PayPal and so on), never a plain form on your site.

07 **Ask your developer, in writing,** where customers' details are stored, who can get at them, when the last backup was made and when the updates were last done.

IF YOU THINK SOMETHING'S WRONG

Change the passwords on your web address, hosting and email accounts, turn on two-step login everywhere, and get someone who understands the code to look at it. If customers' details may have leaked, the ICO's guidance on reporting a breach is at `ico.org.uk`. Remember the 72 hours start when you find out.

FREE HELP

The National Cyber Security Centre's small business guide, at `ncsc.gov.uk`, is short, plain and free. It's well worth half an hour whoever built your site.

08 THE CHECKLIST

Take this to the meeting

Print this page and tick it off as you go. If you can't tick a box, ask why.

Ownership

- [ ] The web address will be in my name, in my own account
- [ ] The hosting or builder account is mine, or it's in writing
- [ ] I'll get a copy of the site and a list of every login
- [ ] I stay primary owner of my Google Business Profile
- [ ] It's in writing what happens if we part ways

Security

- [ ] They explained how customers' details are kept safe
- [ ] Secret keys and passwords stay on the server
- [ ] Admin logins have two-step verification
- [ ] Forms have spam protection and check what's typed
- [ ] Backups are automatic, and someone has tested one
- [ ] Someone is responsible for updates, in writing
- [ ] Card details go to the payment company, never my site

The law

- [ ] A privacy notice written for my site, with a way to complain
- [ ] Cookies and trackers handled properly
- [ ] My business details on the site
- [ ] Accessibility checked against WCAG 2.2
- [ ] If selling: prices include VAT and any fees, and cancelling is explained
- [ ] No made-up reviews or placeholder testimonials
- [ ] Every photo and font is licensed
- [ ] I've checked whether I need to pay the ICO fee

The developer

- [ ] I've seen live sites they built
- [ ] I've spoken to one of their past clients
- [ ] The quote lists every yearly cost
- [ ] They explained anything I asked in plain English

IF YOU'RE NOT SURE

Write to me. A second opinion is free, and you don't need to be hiring me.

If a quote doesn't feel right, or you're worried about the site you've already got, send me the link. It's just me here, so the reply comes from me, and I'll be straight with you.

robert@tideswell.dev tideswell.dev

And if you'd like it built properly, that's what I do, here in Lincolnshire. The web address and hosting are in your name, so the website's yours to keep whatever happens.

WEBSITES

Web design

Built for phones first, set up for Google, and easy to update yourself. Online shops and bookings too.

TILLS

EPOS and tills

A till that handles your stock, use-by dates, rota and cash-up as well. No monthly fee.

SOFTWARE

Custom software

Swap the spreadsheets and paper forms for one system the whole team can use.

Whoever you choose, I hope you end up with a website you're proud of.

Feel free to pass this guide on to anyone it might help. Edition 1, October 2026. Facts and rules were checked in October 2026, but they change. This guide is general information, not legal advice. Sources: Veracode, 2025 GenAI Code Security Report (July 2025); Spracklen and others, "We Have a Package for You!", USENIX Security Symposium 2025; GitGuardian, The State of Secrets Sprawl 2025.

Tideswell has no tide. It's a village in the Peak District, nowhere near the sea, and the name means *Tidi's well*. There is a well, as far as anyone knows.

Robert
Tideswell

FL(2) 5S

