

2027

A FREE GUIDE FROM PIKYHOST

The 2027 Digital Trends Guide

Faster Foundations, Trusted Experiences

Nine shifts shaping websites and online stores across the Gulf, Egypt and Libya — with the numbers, their sources, and three actions after every chapter. Four of them have deadlines inside 2027 itself.

Hosting, building and managing websites,
stores and servers since 2008.



Before You Start

This guide is for whoever actually carries the decision: the owner, the marketing lead, the person answerable for an online store. It is not written for an infrastructure engineer. You need no technical background to read it, and you will finish it holding a list of technical decisions you can explain the reason for.

The markets it covers are the six GCC states (Saudi Arabia, the UAE, Qatar, Kuwait, Bahrain and Oman), Egypt and Libya. Three of the nine chapters change completely depending on which of those you sell in: e-invoicing, data protection and payments. Each of those three carries a **country-by-country table**, and each one says plainly where no published data exists at all.

What is not in here. No broad predictions of the "AI adoption will increase" sort. No advice that would have been just as true in 2023. Every shift below has either a **date it begins** or a **published number** behind it, and four of the nine have deadlines inside 2027.

Our rule on numbers. Every figure comes from a published source, named at the back with the date we read it. Where we could not find a source, we left the number out and said the thing without it. Where a figure is a **forecast** rather than a measurement, it says so and names whose forecast it is.

How to use it. Reading takes about twenty-five minutes. Every chapter ends with three short actions, and there is a 30/60/90-day plan at the back that collects them. Start on the next page. It has four dates on it, and if one of them applies to you, that is the chapter to open first.

Contents

Part One — Nine shifts shaping 2027

1. Search moved from ranking to being quoted
2. Speed became the tiebreaker
3. TLS certificates drop to 100 days
4. E-invoicing spreads across the region
5. Data protection: eight countries, eight different situations
6. Email became infrastructure with admission rules
7. Payment is shifting underneath your store
8. AI agents have started buying instead of customers
9. End of support became the security hole

Part Two — Practical appendix: How to choose a hosting provider in 2027

- Step zero: work out what you actually need
- The four types, and when to move between them
- Twelve questions to ask before you pay
- Five traps in pricing and contracts
- A blank comparison sheet to fill in yourself
- How to read an uptime promise honestly
- A migration plan with no downtime

Closing — the 30/60/90-day plan **Sources**

2027 On One Page

Four published deadlines fall inside this year. Every one of them has a date written down in a published document. None of these is a forecast or an estimate:



Sources: CA/Browser Forum · UAE Federal Tax Authority · php.net — accessed 16 September 2026

Read the timeline like this. The first date has already gone by the time this guide reaches you. If your site is still on PHP 8.2, you are running today on a version that will never receive another security fix. The three dates in the middle need work that **starts months earlier**, not work that starts on the day.

The date this timeline doesn't show

Appointing an accredited service provider for UAE e-invoicing was due **30 October 2026** for large businesses and **31 March 2027** for everyone else. The deadline that actually binds you fell months before the announced one. That pattern repeats in almost every chapter here.

And these dates are not the same in every country. Oman's data protection law came into full effect on **5 February 2026**. Qatar's Council of Ministers approved its draft e-invoicing law on **6 May 2026**. Chapters 4 and 5 take all eight countries one by one, because the gaps between them are wide enough to change your plan completely depending on where your customers are.

PART ONE

Nine Shifts Shaping 2027

Every chapter here has either a date it begins or a published number behind it — and not one of them shows up in your dashboard on its own.

01



Search Moved From Ranking to Being Quoted

What changed

For twenty years the equation was simple: publish content, rank, receive a visitor. The last step broke. Search engines now answer inside the results page itself, so the searcher gets what they came for without clicking anything.

This is not a ranking problem. You can hold position one and lose more than half your traffic, because an AI-generated summary sits above you and tells the searcher what they would have read on your page.

68%

of searches end with no click at all

On mobile that rises to 77%

58–61%

drop in clicks on the top organic result when an AI summary sits above it

Two independent measurements

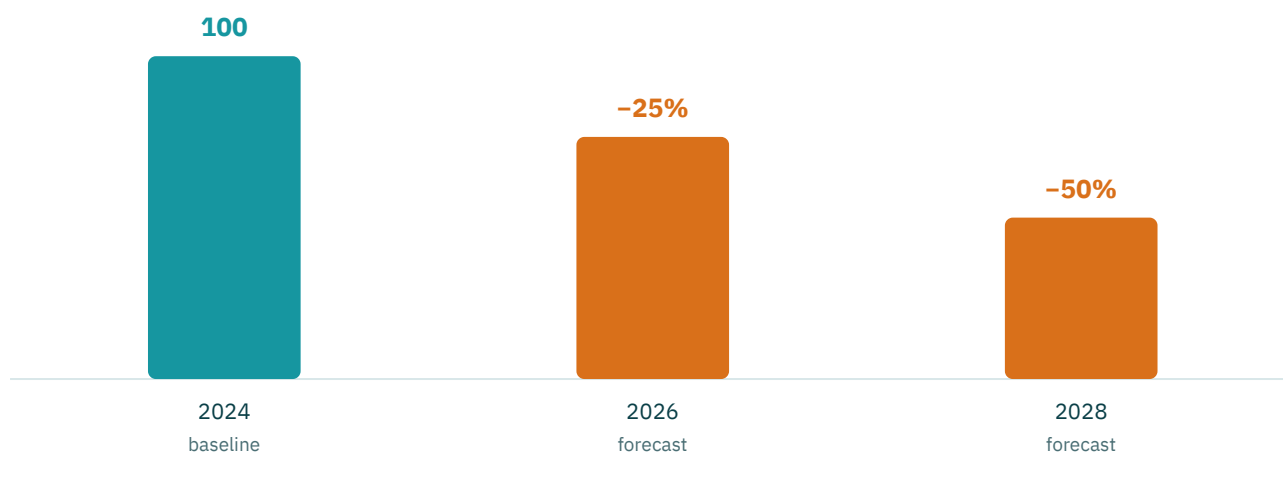
38%

fall in Google referral traffic to content sites in one year

Where the number is heading

The next chart is a forecast, not a measurement. We name whose forecast it is, because that difference matters:

Traditional search volume index — Gartner forecast (2024 = 100)



A published Gartner forecast for traditional search volume and organic traffic — not a measurement of what happened. It is here because it is the number most companies are planning against, not because it is certain.

AI search platforms are forecast to reach **1.2–1.7 billion monthly users in 2027**. The size isn't the interesting part. What matters is that **citation share**, meaning how often your name turns up inside the answer itself, has quietly started replacing ranking as the number worth watching.

What it means for you

If you sell a service: content that used to bring traffic now brings mentions. The goal moved from "be the first link" to "be the source that gets quoted." Your name inside the answer is worth more than your link underneath it.

If you sell a product: buyers arrive having already read a comparison you didn't write, holding an opinion about your price that came from sources you don't control. Your page used to be where they started. Now it's where they check.

Either way, everything you own outright just went up in value: your site, your list, your WhatsApp number, the customers you already have. Nothing sits between you and them, summarising what you said.

A worked example

A site takes 10,000 visits a month from search and converts 2% of them. That's 200 leads. Now half those visits stop happening, because the answer shows up in the results page instead. The site is on 100 leads. Nobody made a mistake and nothing slipped a position.

Doubling your content output won't get those back. Two things will: converting more of whoever still arrives, and owning a channel that doesn't route through a search engine at all. A faster page. A simpler form. A list that is actually yours.

Do this now

- ☐ **Compare the last six months of search clicks against the six before them.** Clicks down while impressions held steady or rose? Then this chapter is describing your site. It is not a penalty and you have not lost a ranking.
- ☐ **Make the pages quotable.** Answer in the first paragraph. Attribute every number. Mark up the structured data. Put a real company, a real address and a real phone number on your About page.
- ☐ **Build one channel you own.** A single email capture point is enough, as long as you are offering something worth an address. Read Chapter 6 before you send anything: the rules for sending changed too.

2

Speed Became the Tiebreaker

What changed

Speed is no longer something a developer brags about. It's a published metric, with numeric thresholds, measured on your real visitors rather than on a test machine.

Google tracks three signals and only calls a page "good" if it passes all three for **75% of its actual visitors**. Your average doesn't matter to it. The slowest quarter of your audience does.

The thresholds you're measured against

Metric	What it measures	"Good" threshold
LCP	When the largest element appears	Under 2.5 seconds
INP	How long the site takes to respond to a tap	Under 200 milliseconds
CLS	How much the layout jumps while loading	Under 0.1

43%

of sites still fail INP specifically

The metric that replaced the older responsiveness signal in March 2024

75%

the percentile your assessment is calculated at
— not the average

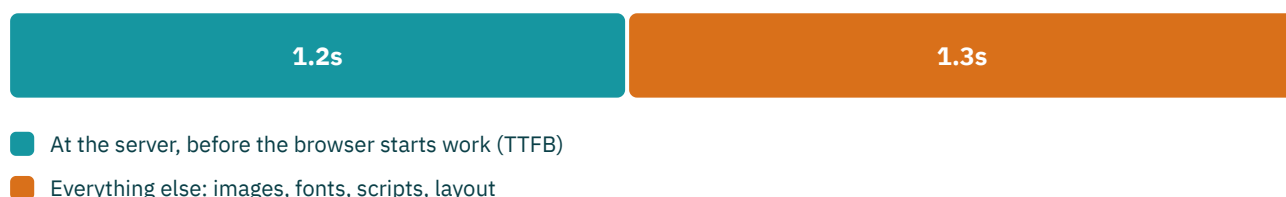
Your slowest quarter decides it

More than 60% of searches happen on a phone, and the assessment is built on the mobile measurement first, even for desktop results. That is why your mobile report always looks worse than you expect. The thresholds were set against a mid-range phone, not against the machine you are reading this on.

Where the two and a half seconds go

This is the part most people miss. You get 2.5 seconds in total, and the first slice of it is spent at the server, **before** anything reaches the browser at all:

A page with a 1.2-second server response — where the 2.5-second budget goes



A worked example illustrating how the budget divides — not a measurement of any particular site.

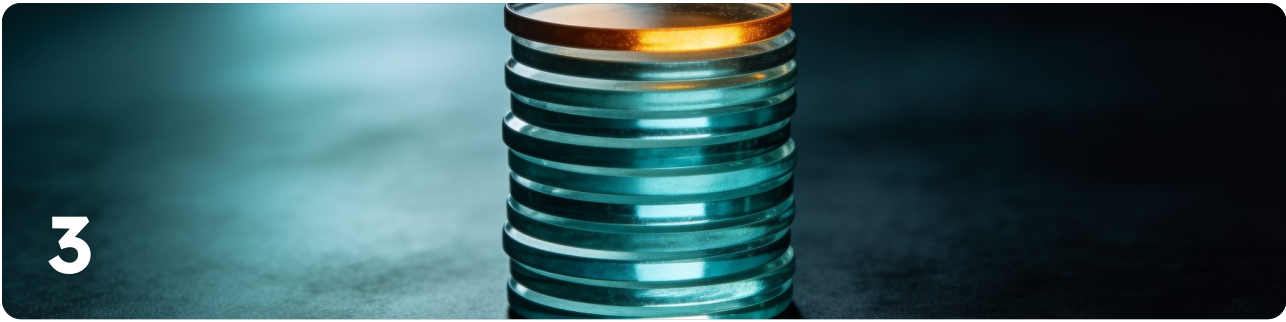
Every 200 milliseconds you save **at the server** comes back doubled, because it widens the budget everything else has to work inside. Your designer cannot give you those milliseconds. Neither can your marketer. They come from the hosting layer: how fast the server answers, how far it sits from your audience, whether there is a caching layer, which PHP version is running, and how many other sites are sharing the machine with you.

What it means for you

Speed has become a **tiebreaker**. Where two pages are close on content and authority, the faster one takes it. It is also the only conversion lever you can pull without asking anyone: no negotiation, no new copy, no ad budget.

Do this now

- ☐ **Measure with field data, not lab data.** Open the page experience report in Search Console instead of running a test tool on your own machine. One of those measures your visitors. The other measures your office internet.
- ☐ Split the problem before you spend on it. High time to first byte means hosting or caching. Low TTFB with a high LCP means images, fonts and scripts. They are different bills.
- ☐ **Start with the three cheapest fixes:** turn on server-level caching, serve modern image formats with their dimensions declared in the markup, and hold back every non-essential third-party script until after the visitor interacts.



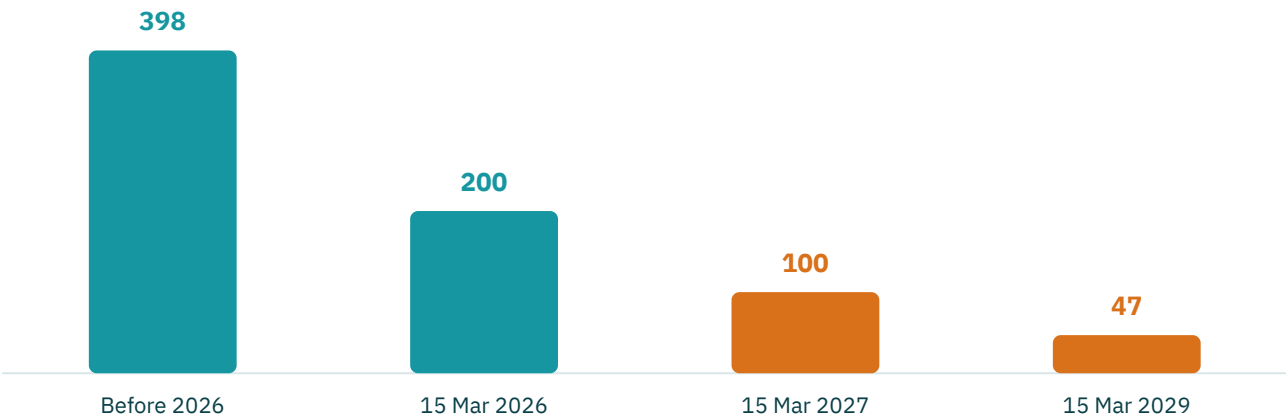
TLS Certificates Drop to 100 Days

What changed

This is the most precisely dated change in the guide, published on a calendar since April 2025.

The body that governs TLS certificates (the CA/Browser Forum) approved a schedule that cuts certificate lifetimes in stages. **2027 is the year the limit falls to 100 days:**

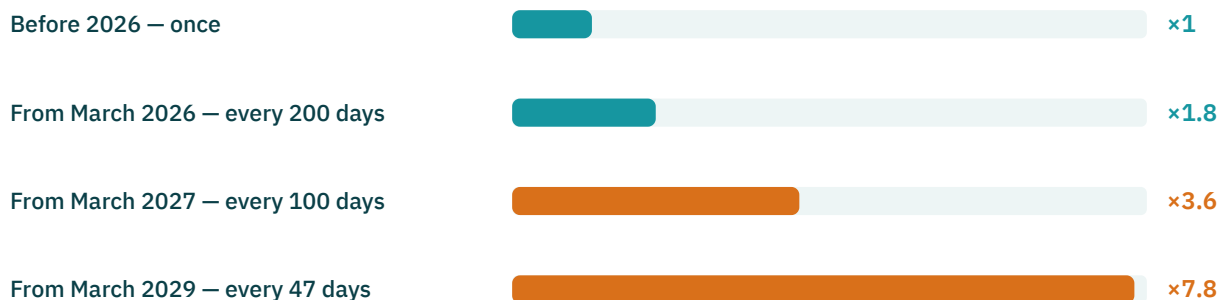
Maximum allowed lifetime of a new TLS certificate (days)



Source: CA/Browser Forum — Ballot SC-081v3, passed 11 April 2025.

In parallel, the period a certificate authority may reuse your proof of domain control shrinks from 398 days to 200, then **100 days in 2027**, then 10 days in 2029. Re-verifying domain ownership accelerates at the same rate.

How many times you renew each certificate per year



Direct arithmetic: $365 \div$ the published maximum for each stage. The published limits are 398/200/100/47 days.

What it means for you

The risk here is operational, not really a security one. An expired certificate doesn't slow your site down. It stops it. Visitors get a red warning page telling them the connection isn't secure, and most of them close the tab. Put that certificate on a payment gateway or an API and the failure is silent instead.

Look at the second chart again. A company that used to renew once a year will renew roughly **four times in 2027**. Run that by hand across ten domains and you have created forty chances a year to forget.

The question that reveals your readiness in thirty seconds

How many live certificates carry your company's name right now? Count the main site, the subdomains, staging, the control panels and the internal tools. Then tell me who gets warned before the earliest one expires.

If you can't answer that, it is the first task of your year rather than the last.

And a second change moving underneath this one

Alongside shorter lifetimes, the move to **quantum-resistant encryption** has started. Browsers went first: Chrome from version 131 and Firefox from 135 already use a hybrid mode combining classical cryptography with a quantum-resistant algorithm. Longer term, the US standards body (NIST) is heading toward **deprecating RSA-2048 and ECC-256 by 2030** and disallowing them after 2035.

None of that asks anything of you today. It does make one question fair game in any hosting conversation: **who updates the encryption layer on my server, me or you?** A company that cannot answer it now will not answer it in 2029 either.

Do this now

- ☐ **Inventory the certificates.** One list. Every domain and subdomain that takes traffic, its expiry date, and the name of whoever owns it.
- ☐ Switch everything you can to automatic renewal, through ACME or whatever your control panel offers. Renewing by hand should become the rare exception you can justify, not the way you normally work.
- ☐ **Ask your host two blunt questions.** First: is auto-renewal on for all my domains, what happens if it fails, and who gets told? Second: who updates the encryption versions on the server? "Of course, it's safe" answers neither.



E-Invoicing Spreads Across the Region

What changed

This chapter is new for 2027, and the reason is simple: **the deadlines land inside the year**. They also differ sharply from one country to the next, which is the part that catches people out.

The regional picture, briefly. Saudi Arabia went first and is four years ahead. The UAE and Oman go mandatory during 2027. Qatar has passed the law but published no schedule. Bahrain and Kuwait are still early. Egypt has been running its system for years. Libya has announced nothing.

Where each country stands (as published up to 16 September 2026)

Country	Status	The date that binds you
Saudi Arabia	Live since December 2021 — two phases (issuance, then integration and near-real-time reporting)	Successive waves reaching smaller revenue bands
UAE	Mandatory in phases, decentralized Peppol PINT model	1 Jan 2027 large · 1 Jul 2027 the rest
Oman	Initiative restarted by agreement in May 2025, Peppol model	Phased launch from 2026, completion expected in 2027
Qatar	Council of Ministers approved the draft law and its regulations on 6 May 2026	No official published schedule. Professional expectation: a phased start around 2027
Egypt	E-invoice and e-receipt systems live and expanding	Successive waves by taxpayer category
Bahrain	Early steps toward implementation	No published schedule
Kuwait	Under study, likely alongside VAT	No published schedule
Libya	No announced mandate	—

"No published schedule" isn't a gap in this table — it *is* the information. Don't plan against a rumour, and check your own tax authority's announcement before any contractual commitment.

The UAE detail, because its deadline is closest

The UAE is implementing e-invoicing in phases on a decentralized model built on the Peppol PINT standard — meaning invoices pass through an **accredited service provider (ASP)** rather than one central system. The dates are published:

UAE e-invoicing phases



Source: the UAE federal e-invoicing framework — accessed 16 September 2026. Check Federal Tax Authority announcements before planning; phases can be amended.

What it means for you

This is not a line item to forward to your accountant and forget about. It is a **technical integration project**, and it reaches into your store:

- **Your store or point-of-sale system** has to produce complete, correctly structured invoice data. Free text will not do.
- **Your master data has to be clean** — tax number, address, item description, unit of measure. Invoices now get rejected over errors the old system shrugged at.
- **The integration needs somewhere to live:** a test environment, keys, monitoring. None of that sits in the accounting software. It sits at the hosting layer.
- **Downtime costs differently now.** A site being down used to mean lost sales. A store that cannot issue a compliant invoice has a compliance problem instead.

The mistake that repeats in every compliance wave

Companies start the month before the deadline. But the deadline that actually binds you is not the mandate date. It is the **date for appointing an accredited service provider**, which falls two to three months earlier. Miss that one and you find the good providers busy and their prices higher.

And if you sell in more than one country

Don't build one integration assuming the countries will converge. Saudi Arabia works on a centralized model reporting to the authority; the UAE and Oman use the decentralized Peppol model through an accredited provider. Those are two different technical paths, not two settings on the same one. **What they share is the data:** item description, tax number, unit of measure, stable identifier. Clean the data once, and treat each country as its own integration.

Do this now

- ☐ **Work out which phase applies to you,** by revenue band and by country, then write down both dates: when you must appoint a provider, and when the mandate starts. Selling in more than one country means one row per country.
- ☐ Ask your developer a single question this week. Can the system we have output an invoice with the required fields, or does it need work? That answer is the difference between a week of effort and three months of it.
- ☐ **Start cleaning the master data now.** Tax numbers, item descriptions, units of measure. It is the longest job on this list, the one everyone postpones, and the one that has nothing to do with technology.

5



Data Protection: Eight Countries, Eight Different Situations

What changed

The most dangerous assumption a multi-market company makes is that "the region" behaves as one unit. In data protection specifically, the gaps between the eight countries are wide enough that the same measure can be mandatory in one and not required next door.

Where each country stands (as published up to 16 September 2026)

Country	Status
Saudi Arabia	PDPL in full enforcement . Fines up to SAR 5 million, and restrictions on transferring residents' data outside the Kingdom
Oman	Law came into full effect 5 February 2026 after a two-year grace period
Qatar	Standalone law since 2017 , amended to move closer to the European model
Bahrain	Standalone law since 2019 , on the same trajectory
UAE	Federal law in force since 2 January 2022 — but its Executive Regulations have not been issued , so practical application stays limited until they are
Egypt	Law No. 151 of 2020 in force
Kuwait	No comprehensive law — a data privacy regulation covers certain telecom providers; a law is anticipated
Libya	We found no comprehensive published law. That is not permission to relax — an enterprise customer asks about your controls regardless of legislation

Read the UAE row carefully: "in force but without executive regulations" does not mean "do nothing." It means the obligation is coming and the detail will be published, and that whoever builds on a sound basis today won't rebuild later.

And Saudi Arabia is the practical lesson

Saudi Arabia's PDPL has moved into full enforcement, with dozens of decisions confirming violations across 2025 and 2026.

SAR 5m

maximum fine for a single violation

Doubled for repeat offences

48

decisions issued confirming violations across 2025 and 2026

×2

penalty doubling on repeat, with criminal liability possible for sensitive-data disclosure

What those decisions were about: processing data with no lawful basis, disclosing it without authorization, missing technical safeguards, and **sending marketing messages without consent**. Note where that last one lands. It is a marketing failure, not an IT one.

Operationally, the clause with teeth is the one on transfers. Moving a Saudi resident's personal data out of the Kingdom is restricted unless you meet specific conditions. That single sentence is why every major cloud provider raced to open a region inside Saudi Arabia.

What it means for you

If you have customers in Saudi Arabia, "where is my customer data physically stored?" is no longer a technical question you forward to a developer. It's a clause in your contracts and a line on the vendor qualification form any enterprise client will send you.

And if you sell to businesses anywhere in the eight, you will be asked before anyone signs. That holds even in the countries with no comprehensive law, because enterprise buyers write their own controls into the contract whatever the legislation says. A company that cannot say where its server sits, and has no processing agreement with its provider, loses deals without ever hearing why.

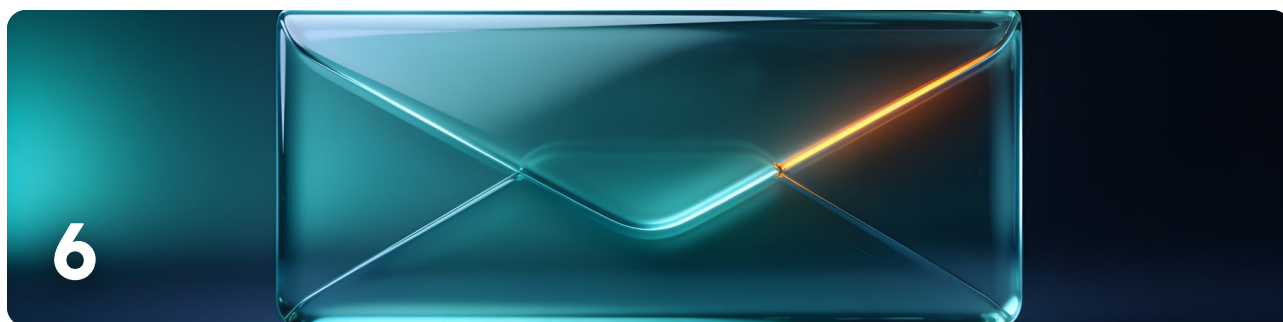
If you operate across several of them, build to the highest bar. Meet the Saudi requirement and you are ready for whatever the UAE publishes later, and for what Oman, Qatar and Bahrain already ask. Build to the weakest country instead and you will simply build it twice.

Three documents you'll be asked for and probably don't have

1. **A Data Processing Agreement (DPA)** with your host, your email provider, and every tool holding customer data.
2. **A location register** for every system holding personal data. Include the backups. Everyone forgets the backups.
3. **Proof of consent** for marketing messages: when this person opted in, which form they used, and how they get out.

Do this now

- ☐ **Write one line per system: where it lives, and who holds the keys.** Site, database, email, backups, analytics, customer files sitting in cloud storage.
- ☐ Ask your host for a written data processing agreement. If they don't already have one to hand, you have just learned something useful about them.
- ☐ **Split the data by country if you need to.** Where your enterprise customers are Saudi, hosting in region is not a performance nicety. It can be a condition of the contract. Write down which country holds which market's data, and put it in the agreement.



Email Became Infrastructure With Admission Rules

What changed

Google, Yahoo, Microsoft and Apple all published conditions for accepting mail, then started enforcing them by refusing messages rather than filtering them. A message that fails the requirements no longer lands in a spam folder. It can be turned away at the door.

The requirements, in short

- Full authentication: **SPF**, **DKIM** and **DMARC**, with domain alignment.
- **One-click unsubscribe** on marketing mail (transactional mail is excluded).
- **A spam complaint rate below 0.3%** — with the practical guidance being to stay under 0.1% and never approach 0.3% at all.
- Sound baseline records for the domain and the sending server.

89%

inbox placement for a sender meeting the requirements

22–34%

of non-compliant mail is routed to the spam folder

A different measure from the first — read each on its own

0.1%

the practical complaint ceiling you should not cross

The formal limit is 0.3%, and recovery from it is slow

What it means for you

This chapter applies to you even if you have never sent a campaign in your life. Your invoice is email. So is your order confirmation, and your password reset. When they stop arriving, the order goes with them.

In 2027 that ties straight back to Chapter 4. Once the invoice is electronic and mandatory, the message carrying it stops being a notification and becomes part of a compliance trail.

Here is the mistake we see most often in this market: **company mail sent from the same server that hosts the website, with no authentication at all.** It works for months. Then a major provider tightens its rules and it stops working, and nothing in any report tells you. The message is not bounced back. It just never arrives.

A five-minute test

Send a message from your company address to a Gmail account and open "Show original." You are looking for three passes: SPF, DKIM, DMARC. Anything less and you are running on luck. Luck gets a shorter shelf life every year.

Do this now

- ☐ **Turn on all three authentication records** for your domain: SPF, DKIM, DMARC. Leave the DMARC policy in monitoring mode at first, then tighten it, so you don't block your own legitimate mail on day one.
- ☐ Keep transactional mail away from marketing mail. An invoice should never be affected by the reputation of a promotional campaign.
- ☐ **Put one-click unsubscribe in every marketing message**, then clear out the addresses that haven't engaged in six months. A smaller list that arrives beats a bigger one that gets refused.

7



Payment Is Shifting Underneath Your Store

What changed

There is no such thing as "the Arab payment method." There are three markets, moving in three directions. Serve all of them from one checkout configuration and you will lose in at least two.

Three markets, three different realities

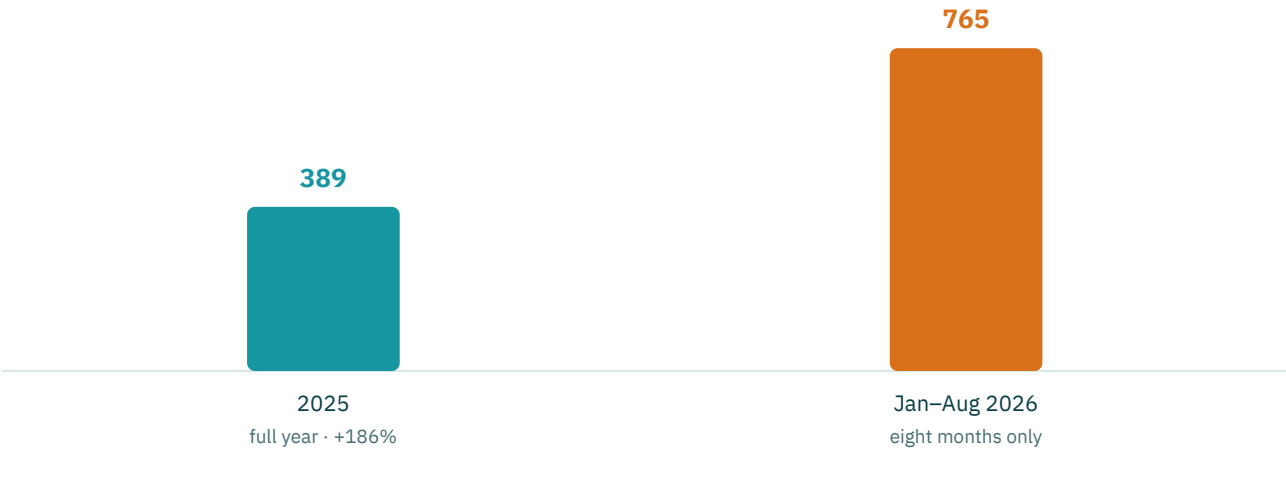
Market	The reality today	What your store needs
Egypt	Cash on delivery is still the largest at about 55% — down from 65% two years ago. InstaPay has passed 16 million users	Cash on delivery + wallet + card, all three
The Gulf	Saudi cash on delivery fell from over 40% a few years ago to roughly 15–20% . The mada network carries over 70% of domestic transactions, and about 36% of shoppers prefer Apple Pay . BNPL adoption is among the highest globally	Wallet and local scheme first · BNPL is a real lever on order value
Libya	A bank-led market growing fast from a low base: 5.5 million activated cards and 4.29 million mobile banking subscribers (February 2026), and 165,313 points of sale	A local gateway on the national switch · don't assume an international card will work

In the UAE the local **Jaywan** scheme is expanding alongside Visa and Mastercard, the global wallets, BNPL providers and instant account-to-account rails.

The scale of the shift in Libya

This figure surprises most people who work the Libyan market assuming it is entirely cash:

Value of electronic payment transactions in Libya (LYD billion)



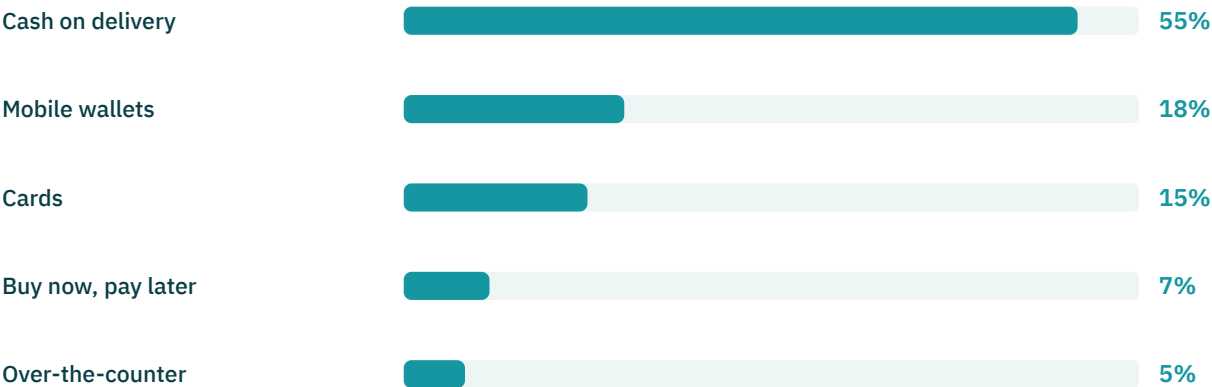
Source: Central Bank of Libya figures as published in local press, September 2026. The two columns are not equal periods — the first is a full year and the second eight months, which makes the gap starker, not smaller.

Internet penetration in Libya is estimated at around **75%**, and there are more mobile subscriptions than people. So the market is not small. It is badly served. Most stores assume Libya is cash-only and give it their weakest checkout, which then proves them right.

And in the Egyptian market

The detailed payment split:

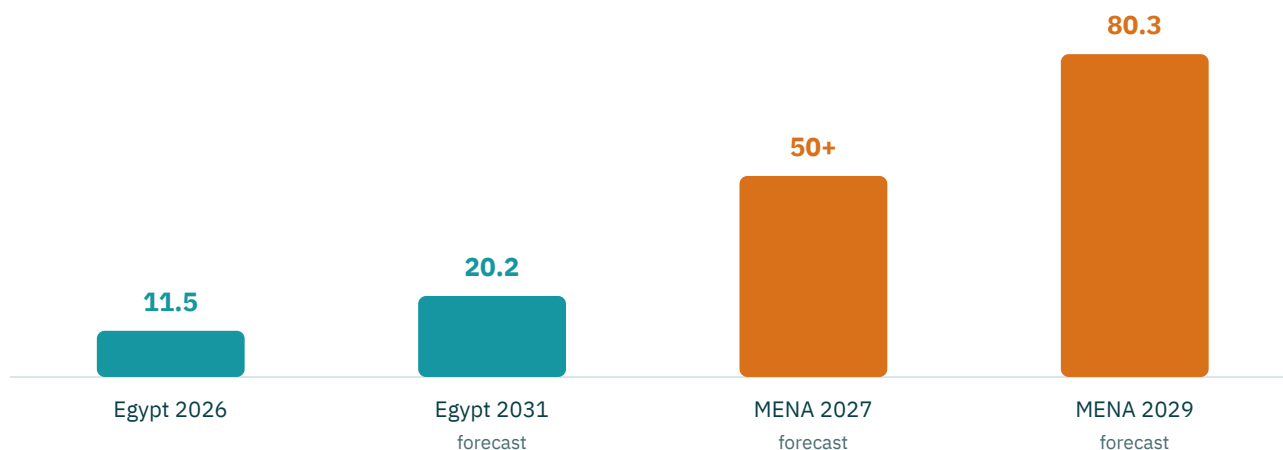
Payment method split in Egyptian e-commerce



Egyptian market payment reports, 2026. Cash on delivery was about 65% two years earlier — the trend is steadily down.

And the market itself is expanding:

E-commerce market size (USD billion)



Egypt: e-commerce market report 2026–2031. MENA: published market forecasts at roughly 11–12% CAGR. Columns marked 'forecast' are not measurements.

What it means for you

Don't build on one method, and don't run one setup across every market. Cash on delivery is still necessary in Egypt, but it is the most expensive option you own once you count returns, wasted shipping and cash that takes weeks to reach you. Make it the default in the Gulf and you look dated to a buyer who is used to paying by wallet in two seconds.

And watch the speed of the payment step itself. Checkout is the one page where the customer has already decided to buy and is standing there waiting. Every extra second, and every payment gateway that fails to load, costs you someone you had already won.

A worked example

A store doing 1,000 orders a month, 55% of them cash on delivery, with a 15% refusal/return rate on those versus 3% on prepaid orders.

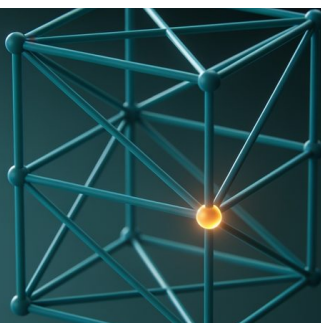
That is roughly **82 lost orders a month**, each one shipped out and back again at your expense. Move ten percentage points of that cash-on-delivery volume to prepaid and you save about 12 of them every month, and shorten your cash cycle while you are at it.

The cheapest way to make that shift is not a discount. It is a familiar payment option that works first time and does not throw the customer out of your store to complete it.

Do this now

- ☐ **Offer at least three methods in every market,** ordered the way that market pays rather than the way your home market does: in Egypt cash on delivery is present but shouldn't be the default; in the Gulf the wallet and the local scheme lead.
- ☐ **Make a real payment yourself from your phone** on mobile data rather than Wi-Fi, and record how many seconds it took from "place order" to the confirmation page. Repeat it with a card from each market you sell into.
- ☐ **Review pending and failed orders weekly.** The thing that most often hides a payment problem is that the store never reports one.

8

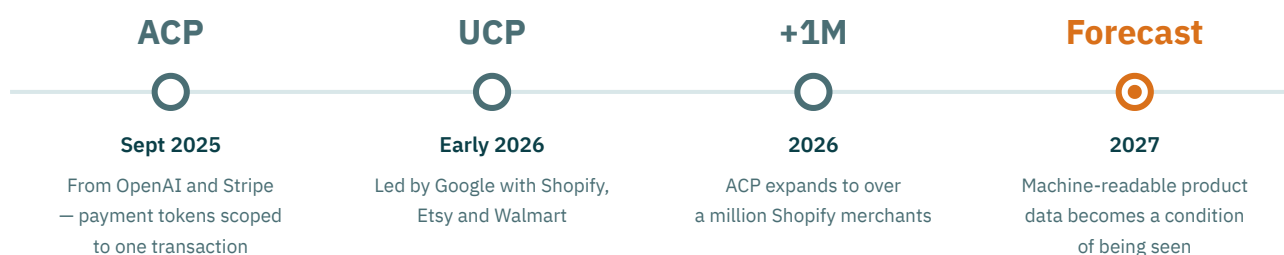


AI Agents Have Started Buying Instead of Customers

What changed

Open protocols now let an AI agent search for a product, compare options, add to cart and complete payment on a user's behalf:

How we got here



The first three are published announcements from the parties themselves. The column marked 'forecast' is a reading of direction, not a certainty.

What it means for you

None of this is far off, and none of it is a reason to rebuild your store this year. What it does ask for is modest, and you want it anyway for other reasons.

Clean, structured product data. Name, description, price, availability, a stable identifier, an image, all in a form a machine can read rather than just an eye. Your paid ads and your search listings already need exactly this. So does Chapter 4: e-invoicing wants an accurate item description, a stable identifier and a unit of measure. Clean the data once and three different problems get smaller.

Technical consistency. An agent does not behave like a person. It does not wait, it does not refresh, and it does not come back in a minute to try again. If your store is slow or throws an error, it moves on to the next store. You will not see that in any report, because the visit never completed.

The practical takeaway

Rebuild nothing. Get the product data right and structured, and make the store answer quickly and consistently. That is enough to be visible to an agent and buyable by one, and it pays you back today rather than in some future year.

Do this now

- ☐ **Review your product structured data** (Product / Offer schema): correct price, correct availability status, and a stable product identifier that doesn't change every time you edit.
- ☐ **Clean the product feed** you send to your ad platforms. It is usually the closest thing you already have to what an agent will read, and to what e-invoicing wants.
- ☐ **Monitor response time and error rate on product and cart pages**, not just the homepage. The homepage is the least relevant page to somebody who is buying.



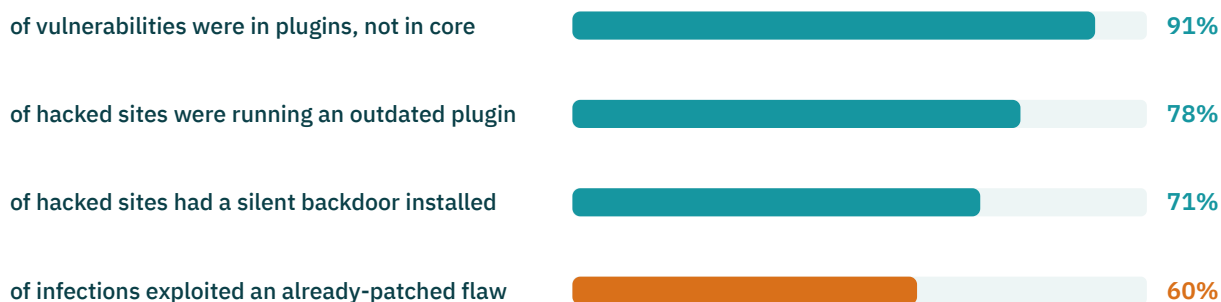
9

End of Support Became the Security Hole

What changed

Most people picture a hack as a skilled attacker choosing them. That is not what happens. What happens is automated scanning at enormous scale, hunting for a known, published, already-patched flaw on a site nobody updated.

What the WordPress ecosystem numbers say



WordPress ecosystem vulnerability reports for 2025: 11,334 vulnerabilities found, up 42% year over year.

Read the last row twice. Sixty percent of infections used a flaw that **already had a fix**. Nobody was outsmarted. Somebody was behind on updates.

And the part specific to 2027

The software your site runs on has published end dates, and 2027 sits in the middle of them:

PHP version end of support



Source: the official PHP release schedule. And the majority of public sites today still run versions whose support has already ended.

A version past end of support is not "a bit slower." It is a version where the next flaw gets found and no fix is ever written. Every compliance check and every cyber insurance questionnaire asks about it by name.

A backup you have never restored is not a backup

The question is not "do you have backups?" It is **when did you last restore one?** How long did that take? And did the database match the files when you did?

Companies that discover their backups are empty always discover it on the worst possible day.

Do this now

- ☐ **Find out which PHP version your site is on today.** One line from your developer, or one look at the control panel. If the answer is 8.2 or older, stop reading and deal with that first: it is the most urgent item in this guide.
- ☐ Pick one update day a week and keep it. If the site earns money, test on staging first. And delete the deactivated plugins and unused themes rather than leaving them switched off, because switched off is still installed.
- ☐ **Restore a backup this month** onto a separate environment and time it. That number is your real recovery time. The one in the contract is a different number.

PART TWO

Practical Appendix: How to Choose a Hosting Provider in 2027

Written to be used, not read. Print it and take it into any sales call.

02

Step Zero: Work Out What You Actually Need

Before comparing plans, write down these six numbers. Most bad hosting decisions start right here: a company buys a plan on a guess, then discovers it's paying for more than it needs or running on less than it takes.

What you need to know	Where to find it	Why it matters
Monthly visits and peak hours	Analytics, last 12 months	The peak is what takes a site down, not the average
Database size	Control panel, or ask your developer	A store with tens of thousands of products is not a blog
File and media size	Size of the site folder	Grows silently and breaks backups
Number of mailboxes and their size	Ask your team	The most forgotten line item, then paid for twice
Where your audience is	Analytics geography report	Determines the right server location
What one hour of downtime costs	Monthly revenue ÷ 720, roughly	Determines how much reliability is worth paying for

The last number is the important one. A business losing the equivalent of a few dollars per hour of downtime should not buy the same solution as one losing thousands.

The Four Types, and When to Move Between Them

Type	Suits	Sign you've outgrown it
Shared hosting	Brochure site, blog, small store	Repeated slowness at specific times, or resource-limit warnings
VPS	Growing store, application, multiple sites	Steady usage above 70% of resources, or a need for custom configuration
Dedicated server	Heavy load, sensitive data, compliance requirements	A need for full isolation, or performance that can't tolerate sharing
RDP / remote desktop	A team needing a shared, always-on work environment	Not a substitute for website hosting — an entirely different purpose

The practical rule: don't move because a salesperson suggested it, and don't stay because moving is frightening. Move when your resource report sits consistently above 70%, or when downtime starts recurring at the same time of day.

Twelve Questions to Ask Before You Pay

Print this page. The difference between a good provider and a weak one shows up in **how clear the answer is**, not how warm it is.

On performance

1. What's the typical server response time for a site like mine, and where is the server located? *A good answer:* a number, a specific location, and a willingness to be tested.
2. Which PHP versions are available, can I change mine myself, and what's your plan for customers still on an end-of-life version?
3. What server-level caching layer is included?
4. Roughly how many sites share my server? *Bad sign:* refusing to answer, or "that doesn't matter."

On continuity

5. What uptime is guaranteed in writing, and what's the remedy if it's missed?
6. How often are backups taken, how many are kept, and where do they sit: on the same server, or off it? *Bad sign:* backups on the same server only. If the server goes, they go with it.
7. Can I restore a backup myself without opening a support ticket, and how long does it take?
8. What happens if a TLS certificate expires or auto-renewal fails, and who gets notified? And who updates the encryption layer on the server?

On the relationship

9. What support channels exist, what are the real hours, and what's the actual average response time?
10. Who performs my migration, is there a cost, and what downtime should I expect?
11. Is there a data processing agreement (DPA), and who on your side can access my data?
12. What is the renewal price after year one? Give me the figure, not the percentage.

Five Traps in Pricing and Contracts

1. **The first-year price is not the price.** Many offers are compared on a one-off promotional rate that doubles on renewal. Always compare on the **second-year price**, and write it into the comparison sheet.
2. **"Unlimited" always has a limit.** Unlimited storage and unlimited transfer are in the ad and limited in the fair-use policy. Ask for the actual figure at which throttling begins — and get the answer in writing.
3. **Backups may be a paid add-on.** Plenty of businesses discover on the day they need it that backup was an optional extra they never bought. Ask plainly: included, or add-on?
4. **The refund policy has exclusions.** It usually doesn't cover domains, licences or certificates. Read the exclusion before you read the promise.
5. **Who owns the domain?** The domain must be registered **in your company's name**, under an email address you control. A domain registered to an agency or a former employee is the most dangerous invisible item in any technical setup, and you only discover it on the day of a dispute.

A Blank Comparison Sheet

Fill this in for three providers. Compare on objective criteria you choose, not on anybody's general verdict.

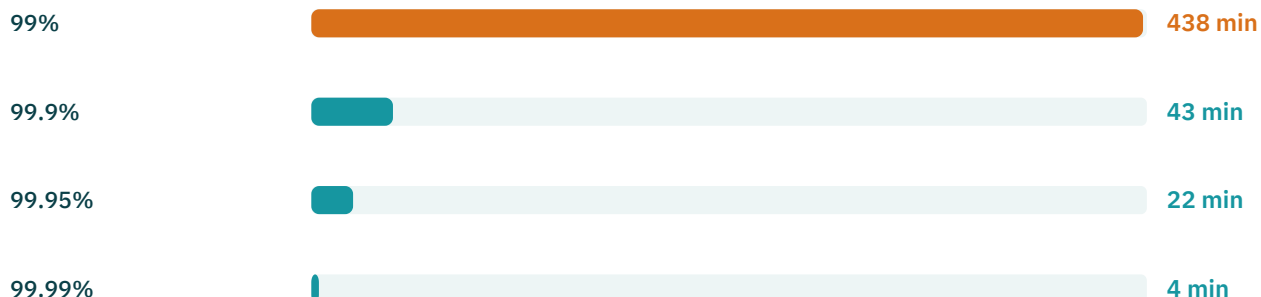
Criterion	Provider A	Provider B	Provider C
First-year price			
Renewal price			
Server location			
Measured response time			
PHP version and self-service change			
Server-level caching			
Backup frequency			
Where backups are stored			
Self-service restore?			
SSL and automatic renewal			
Mailboxes included			
Uptime guaranteed in writing			
Support response time (measured, by test)			
Migration included?			
Data processing agreement			

A free test before you buy: send a moderately technical question to each provider's support on an ordinary working day, and record how long the reply took and how useful it was. That's the most accurate piece of information you'll get, and it costs you five minutes.

How to Read an Uptime Promise Honestly

"99.9%" looks close to perfect. Here's what it actually means, in minutes per month:

Allowed downtime per month at each uptime level (minutes)



Direct arithmetic on a 30-day month. Per year: 3 days 15 hours · 8 hours 45 minutes · 4 hours 23 minutes · 52 minutes.

The two questions that reveal how serious the promise is:

1. Is scheduled maintenance excluded from the calculation? Usually it is, and that changes the number considerably.
2. What is the remedy, and is it credited automatically or does it require you to claim it within a set window?

A Migration Plan With No Downtime

Moving between providers isn't risky in itself. The risk is in the order of the steps.

1. **Lower your domain's TTL** to 300 seconds a full day before the move. Do this before anything else.
2. **Copy everything** to the new server: files, database, and mailboxes with their contents.
3. **Test on the new server before switching**, using a hosts file or a temporary domain. Browse it as a visitor would: homepage, a product, the cart, a contact form, and login.
4. **Freeze changes** on the old site during the switch, so data doesn't split across two servers.
5. **Switch the domain**, then watch both servers for 48 hours. Mail often lags behind the website.

- 6. Once stable:** enable the certificate and auto-renewal, reconfigure the mail records (SPF/DKIM/DMARC) for the new environment, confirm backups are running, then set TTL back to normal.
- 7. Don't cancel the old account for two weeks.** It costs one more billing period, and it buys you a way back.

Closing: The 30/60/90-Day Plan

Don't implement the whole guide. Implement this.

First 30 days — find out where you stand

- ☐ Find out which PHP version your site runs (Chapter 9)
- ☐ Inventory your TLS certificates and their expiry dates (Chapter 3)
- ☐ Identify which e-invoicing phase applies to you, and write both dates (Chapter 4)
- ☐ Check your email authentication in five minutes via "Show original" (Chapter 6)
- ☐ Open the page experience report and record all three metrics on mobile (Chapter 2)
- ☐ Compare search clicks over the last 6 months to the 6 before (Chapter 1)

The next 60 days — close the cheap gaps

- ☐ Upgrade PHP to a supported version, after testing on a separate environment (Chapter 9)
- ☐ Enable automatic certificate renewal on every domain (Chapter 3)
- ☐ Enable SPF, DKIM and DMARC, and separate transactional from marketing mail (Chapter 6)
- ☐ Turn on server-level caching, and fix images and scripts (Chapter 2)
- ☐ Set a weekly update day, and delete every unused plugin and theme (Chapter 9)
- ☐ Actually restore a backup, and record how long it took (Chapter 9)

By 90 days — build what doesn't depend on anyone

- ☐ Clean your master data: item descriptions, tax numbers, product identifiers (Chapters 4 and 8)
- ☐ One email capture point on the site with a genuine reason behind it (Chapter 1)
- ☐ At least three payment methods per market, with a real test payment from your phone (Chapter 7)
- ☐ A written data processing agreement with your host (Chapter 5)
- ☐ Fill in the comparison sheet for three providers, even if you end up staying where you are (Appendix)

One Last Thing

Every shift in this guide has one thing in common. **None of them shows up in a report.** The certificate expires and the site stops. The email gets refused and never bounces back to tell you. The breach runs quietly for months. The AI agent leaves without registering a visit. An end-of-life PHP version works perfectly, right up until the day it doesn't. Nothing in your dashboard turns red for any of it.

That is why the whole 30-day plan is **measurement** rather than building. Find out where you stand first. Most of what you turn up will be cheaper to fix than you feared.

Want a second opinion?

PikyHost offers a **free technical check** on one site: server response time, the three speed metrics as your real visitors experience them, certificate status and expiry date, email authentication, and PHP and plugin versions that are out of date.

A written report with your own numbers — not a sales deck.

pikyhost.com · Hosting, building and managing websites, stores and servers for businesses across the Gulf, Egypt and Libya since 2008.

Sources

Every figure in this guide comes from a published source. All sources accessed **16 September 2026**. Anything described as a "forecast" is a published projection from a named party, not a measurement of what happened.

Chapter 1 — Search and citation

- Search Engine Land — Google zero-click search study, early 2026
- Ahrefs and Seer Interactive — independent measurements of AI Overview impact on click-through rate
- Gartner — forecast of a 25% drop in traditional search volume by 2026, and a 50% fall in organic traffic by 2028
- Published forecasts of AI search platform users through 2027

Chapter 2 — Core Web Vitals

- Google Search Central / web.dev — LCP, INP and CLS thresholds and the 75th-percentile method
- Public CrUX data on INP failure rates

Chapter 3 — Certificate lifetimes

- CA/Browser Forum — Ballot SC-081v3, passed 11 April 2025
- DigiCert — explanation of the certificate lifetime reduction schedule
- NIST IR 8547 — timeline for deprecating RSA-2048 and ECC-256
- Chrome and Firefox release notes on hybrid post-quantum key exchange

Chapter 4 — E-invoicing

- The UAE federal e-invoicing framework and its published implementation phases
- Zakat, Tax and Customs Authority (ZATCA) — Saudi e-invoicing rollout phases
- Oman Tax Authority — announcement of phased implementation on a Peppol model
- Qatar Council of Ministers — approval of the draft e-invoicing law and regulations, 6 May 2026
- Egyptian Tax Authority — e-invoice and e-receipt systems
- Published professional reviews of the Bahraini and Kuwaiti positions (early stage, no announced schedule)

Chapter 5 — Data protection

- Saudi Data and AI Authority (SDAIA) — Personal Data Protection Law and 2025–2026 enforcement decisions
- UAE Federal Decree-Law on personal data protection, in force since 2 January 2022 (Executive Regulations not yet issued)
- Qatar (2017) and Bahrain (2019) personal data protection laws
- Oman personal data protection law — in full effect from 5 February 2026
- Egypt — Personal Data Protection Law No. 151 of 2020
- Published regional legal reviews of the Kuwaiti position (no comprehensive law as of the access date)

Chapter 6 — Email admission rules

- Google Workspace Admin Help — Email sender guidelines (bulk sender requirements)
- Yahoo, Microsoft and Apple sender guidelines, 2025–2026 updates

Chapter 7 — E-commerce and payment

- Mordor Intelligence — Egypt e-commerce market report, 2026–2031
- Egyptian market payment-method reports, 2026 (wallets, cards, BNPL)
- MENA e-commerce market forecasts through 2029
- Central Bank of Egypt — InstaPay figures
- Saudi and UAE payment-method reports, 2026 (mada, Jaywan, wallets, BNPL, cash on delivery)
- Central Bank of Libya — electronic payment indicators for 2025 and 2026 as published in local press
- Estimates of internet penetration and mobile subscriptions in Libya, 2026

Chapter 8 — Agentic commerce

- OpenAI and Stripe — Agentic Commerce Protocol (ACP), September 2025
- Universal Commerce Protocol (UCP) — joint announcement, early 2026

Chapter 9 — Security and end of support

- Annual WordPress ecosystem vulnerability reports for 2025 (Patchstack / WPScan)
- php.net — supported versions and end-of-support dates

If you find a figure you believe has changed since the access date, tell us. We review this guide every three months.



Start by measuring, not by building

Most of what you find will be cheaper to fix than you expected. Start with the 30-day plan at the back of this guide — all of it is measurement.

A free technical check on one site: server response time, the speed metrics as your real visitors experience them, certificate status and expiry, email authentication, and out-of-date PHP and plugin versions. A written report with your own numbers — not a sales deck.

pikyhost.com