interweb

Generated on 21/10/2026 17:20

KNOWLEDGE BASE · PUBLIC DOCUMENT

Selling online: PCI, card data and what shared hosting is not

Security

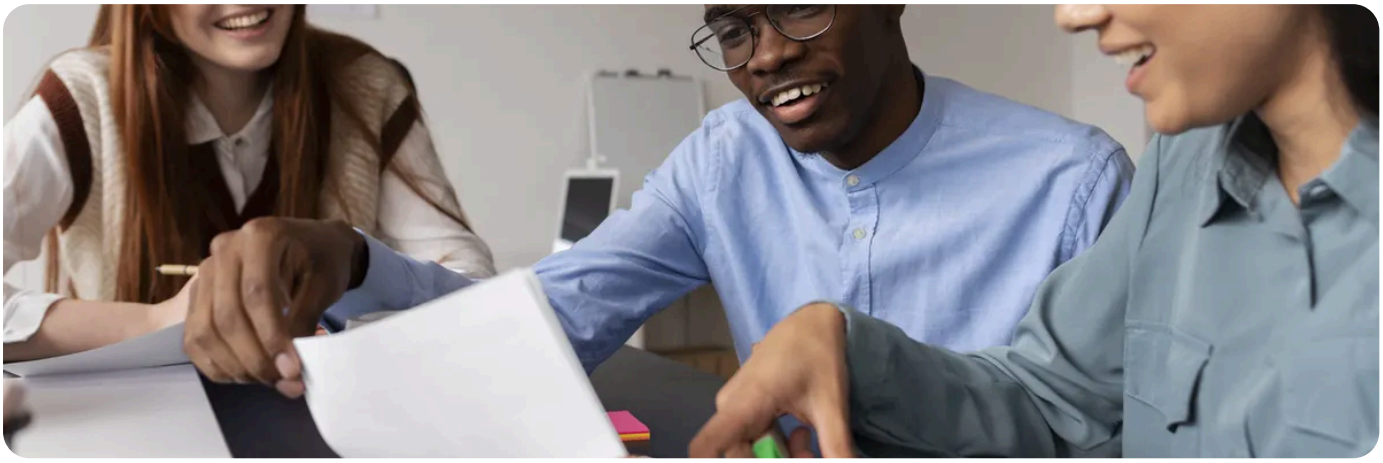
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-328	v2026.09.28	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/328

Selling online: PCI, card data and what shared hosting is not

Security Created on **September 11, 2026** Updated on **September 28, 2026** 4 min read



Anyone setting up a shop eventually arrives at this question, often because a bank or a corporate customer asked it first: *is your hosting PCI compliant?* The honest answer has two parts, and the second one is good news.

The direct part

We do not hold PCI DSS certification, and shared hosting is not sold as a certified environment. The same applies to regimes such as HIPAA in healthcare. We do not say this lightly: we would rather you knew before building the business than found out during an audit.

This is not a shortcoming of the service. A PCI-certified environment is an **audited certification of the whole chain** - hardware, network, processes, people and logs - and on shared hosting, by definition, the machine belongs to many. No serious provider certifies a shared plan, and anyone claiming otherwise deserves a follow-up question.

The good news: almost no shop needs it

PCI DSS applies to anyone who **stores, processes or transmits card data**. And the way out is simple: **do none of those things**. That is how the overwhelming majority of online shops you know actually work.

How you take payment	What it means for you
The customer leaves for the bank or gateway page	Card details never pass through your site. Your PCI scope drops to the simplest questionnaire there is.
Gateway form embedded in your page	The fields belong to the gateway, not to you. The data goes straight to them. You stay in the simplest regime.
Mobile money or bank reference	There is no card involved at all. PCI does not apply.
Your site receives and stores the card number	**Do not do this.** You take on real audit obligations, and legal liability if there is a breach.

The golden rule, if you take one thing from this article.

Never store card numbers - not in the database, not in a file, not in an e-mail, not in a spreadsheet, and not «just the last four digits plus the expiry». If your developer says they need to keep them for something, get a second opinion: the gateway almost always solves it with a *token*, which lets you charge again without ever holding the number.

What we provide, and how it helps

None of this is a certification, but it is the ground a secure shop is built on:

What	What it is for
Encrypted connection (SSL/TLS)	Automatic certificate on every domain in the account - see **what is an SSL certificate**. Force HTTPS across the site: **how to force HTTPS**
Isolated accounts	Each hosting account is kept separate from the others on the same server.
Current PHP versions	You can pick a version that still gets security support - and you should: **how to change your PHP version**
Backups	Confirm what your plan includes and know how to restore before you need to - **restoring data with JetBackup**

And what stays yours

This part does not come with the hosting, and it is where shops with problems fall down:

1. **Keep the shop updated.** Platform, theme and extensions. A known hole in a payments plugin is how they get in.
2. **Choose a proper gateway** and use its official integration - not an old module found on a forum.
3. **Control who has access.** One administrator account per person, passwords different from personal ones, and **healthy suspicion of e-mails that look like ours**.
4. **Do not keep what you do not need.** That goes for cards and for customer data generally - see **personal data protection: what applies to your website**.

Where our work ends and yours begins is written in **how far our support goes**. If you suspect the shop has been tampered with, **how to tell if your site has been compromised**.

And if you genuinely need a certified environment?

It happens: there are contracts, tenders and banking partners that require it in writing. In that case the route is not a shared plan - it is a **server of your own**, VPS or dedicated, configured for the purpose and **audited by a qualified body**. Certification is a process with a cost and a timescale, not a product you add to a cart.

We can supply the machine and work with whoever runs the audit. What we will not do is declare compliance we do not hold. For who handles what on your own server, see **managed or unmanaged VPS**; for keeping it locked down, **keeping your VPS secure**; and for which jump is right, **shared hosting vs VPS**.

Before you assume you need it.

Plenty of people ask for «PCI hosting» because they were told to, when in fact they already use a gateway and never touch card data at all. Tell us how you take payments and we will help work out which case you are in - it may save you a server you do not need.

NEED A HAND?

Going to sell online and unsure what you need?

Talk to us →

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-328 · v2026.09.28 · Generated on 21/10/2026 17:20