Before you share that link — run through this list.

Built for low-stakes customer-facing apps: ROI calculators, configurators, assessment tools, and portals. Not for apps handling payments or sensitive PII — those need a developer review.

1. DATABASE & DATA

- [ ] **Row Level Security (RLS) is ON**
  EverySupabasetable musthaveRLSenabled. The #1 missed step in Lovable apps.

- [ ] **No RLS policy set to "true"**
  Apolicy ofusing(true)opens your database to everyone. Reject it unless you explicitly want public access.

- [ ] **No service-role key in frontend code**
  ServicekeysbypassRLS entirely.Theybelong in Edge Functions only — never in browser-accessible code.

- [ ] **Only public-safe keys in the frontend**
  The SupabaseanonkeyandStripepublishable key are safe client-side. Everything else goes behind a backend proxy.

2.AUTHENTICATION

- [ ] **Protected routes actually redirect**
  Openeveryprotected pagein aprivatebrowser window without logging in. You should land on the login page, not the content.

- [ ] **Users can only see their own data**
  Log inas twotest users.ConfirmUserAcannot access User B's records or account details.

- [ ] **Password breach protection enabled**
  Lovable Cloud:Settings Auth EnableHIBPCheck. Blocks known compromised passwords.

3. PROJECT SETTINGS

- [ ] **Project is set to Private**
  ProjectSettings Visibility Private. Public projects expose your source code and chat history to other Lovable users.

- [ ] **Lovable's Deep Scan is clean**
  Security DeepScanbeforepublishing. Fix all flagged items. Free.

- [ ] **No sensitive data in project name**
  Project names canbe visible.Don't include customer names, system names, or anything confidential.

4. FUNCTIONAL QA

- [ ] **Tested on mobile**
  Openona phonebefore sharing. Lovable apps are responsive by default, but always confirm.

- [ ] **Tested in a private/incognito window**
  Clears cachedsessionsandshowsexactlywhat a new visitor sees.

- [ ] **Form submissions actually work**
  Fill outandsubmiteveryform.Confirmdata lands where it should and confirmations appear.

- [ ] **No broken links or missing images**
  Clickeverybutton andlink. Dead endsandmissing assets make your business look unpolished.

5. BRANDING & LEGAL

- [ ] **Privacy notice present if collecting data**
  Ifthe appcollectsaname, email, or anyinput— you need a privacy statement. What you collect, why, and who to contact.

- [ ] **Your logo and branding applied**
  ReplaceLovable'sdefaultstylingwithyour company name, logo, and colors. First impressions matter.

- [ ] **No Lovable branding visible to users**
  Check thebrowsertab title,favicon,andfooter text. Update these in Project Settings.

- [ ] **Contact info or next step is clear**
  Every customer-facingapp should answer "what do I do next?" Don't leave visitors at a dead end.

6. GOVERNANCE

- [ ] **Someone in IT or ops knows this exists**
  ShadowAIisthenewshadowIT. Loopintheright person before sharing externally — even for low-stakes tools.

- [ ] **You know who owns it going forward**
  Whoupdatesitwhensomethingbreaks?Decide before launch, not after.

- [ ] **You're not storing customer PII**
  Names,emails,or phonenumbers require additional compliance steps. If in doubt, don't store it.

7. LOVABLE'S BUILT-IN TOOLS

Lovable includes free security tools — use them every time:

- **Security Basic Scan** runs automatically before every publish
- **Security Deep Scan** analyzes your full codebase on demand
- **Dependency checks** run continuously in the background

8. SLOPSQUATTING WATCH

What is slopsquatting?

AI tools recommend non-existent packages ~20% of the time. Attackers register those fake names with malicious code — when your app installs them, the attacker gets in. Lovable's dependency checks catch most cases. Always confirm Deep Scan shows zero dependency warnings before going live.

- [ ] **Deep Scan shows zero dependency warnings**
  Run before every public launch. Free in the Security panel.

BlueStar Nation

The ADC and POS channel's destination for end-user insights and thought leadership from marketing and sales professionals — data-informed articles for VARs, ISVs, and MSPs. Visit nation.bluestarinc.com to explore more tools, trends, and resources.