

When a law firm website displays “Error establishing a database connection,” visitors may be unable to read practice-area pages, find your phone number, or submit a contact form. The message usually means WordPress cannot communicate with its database. It does not, by itself, prove that data has been lost or that the site has been hacked.

Start with the fastest reversible checks. Record what you see, avoid making several changes at once, and protect a copy of the site before editing configuration files or changing database settings. The goal is to restore service safely, protect leads, and give potential clients a clear way to contact the firm while the website is unavailable.

First: Triage the Outage Without Changing Anything

Before troubleshooting, confirm the scope of the problem. Use a private browser window or a different device and network to load the website. Check the homepage and a few important pages, including the contact page. If the site works for you but not for others, the issue could involve browser caching, DNS, or a network-specific problem rather than a site-wide database failure.

Keep a simple incident scratchpad. Exact wording and times help you identify whether the issue is recurring and give your hosting provider useful evidence.

- Record the date and time, including your time zone.
- Copy the exact error message. Note whether it appears on every page or only some pages.
- Write down what changed recently: a WordPress update, plugin update, password change, migration, or hosting change.
- Note whether the hosting account’s control panel and email are working.
- Take a screenshot, but do not include private client or matter information.

Do not repeatedly refresh a site that is under heavy load, and do not start installing troubleshooting plugins. A plugin cannot repair a database connection that WordPress cannot establish, and new changes can make an outage harder to diagnose.

Put a temporary contact route in place

While investigating, make sure prospective clients can still reach the firm. If you have a reliable, non-technical way to publish a maintenance notice—such as a website host’s status page, a managed maintenance feature, or a separate firm-controlled page—use it. State that the website is temporarily unavailable and give a verified phone number or other approved contact route. Do not promise a response time you cannot meet.

Law firm websites can receive sensitive information through forms. Do not invite visitors to send case details, documents, or confidential information through an unapproved personal email address or social account. If the normal contact form is down, ask visitors to call the firm or use another channel the firm has already approved.

```
    ${this.name}, Version: ${this.
ync function fetchData(url) { try { let res
ow new Error("Network response was not ok")
rn data; } catch (error) { console.error
    { let num = 1; while (true) { yield
        document.getElementById("generat
document.getElementById("number").textContent
        ElementById("calculate").addEventListener
        "calculate", payload: 10 }); }); class Ad
this.fibonacci(n - 1) + this.fibonacci(n
(base, exp); } static factorial(n) { } }
```

Check Whether the Problem Is With Hosting or the Server

A database connection error can be caused by the database server being unavailable, overloaded, or temporarily restarting. It can also follow a hosting incident, resource limit, or scheduled maintenance. Check the hosting provider's status page and account dashboard first. Look for notices about database services, web-server health, resource limits, account suspension, or maintenance.

If you have access to the hosting control panel, look for database status and recent resource or error logs. Do not restart services or alter server settings unless you manage the server and understand the consequences. On managed hosting, ask the provider to verify service health rather than trying to make server-level changes yourself.

Use a specific support request

If the hosting dashboard does not explain the outage, send support a concise report. For example:

"Our WordPress site, [domain], began showing 'Error establishing a database connection' at [time and time zone]. The error is [site-wide / limited to these pages]. The hosting dashboard is [available / unavailable]. We last changed [specific change, or 'nothing known']. Please check whether the database server is reachable, whether this account has hit resource limits, and whether there are database or web-server errors around that time. Please do not restore or modify files or databases without confirming with us first."

This gives the host a clear investigation path while avoiding an unapproved restore that could overwrite recent site content or form records.

Check WordPress Database Credentials Carefully

WordPress reads its database connection details from wp-config.php, typically located in the WordPress installation's main directory. A typo, outdated password, incorrect database name, or mismatched database username can prevent a connection. This is especially worth checking after a migration, hosting change, password rotation, or manual configuration edit.



The relevant settings commonly look like this:

- DB_NAME — the database name.
- DB_USER — the database username.
- DB_PASSWORD — the database password.
- DB_HOST — the database host or server address.

The values must match the credentials and host details assigned by your hosting provider. Do not assume the database host is always localhost; providers may use a different hostname. Also check that the database user has the required permissions for the correct database.

Back up before editing wp-config.php

Before touching the file, create a copy of wp-config.php and store it securely. It contains sensitive credentials, so do not email it, paste it into a public support forum, or share a screenshot that reveals its contents. Use your host's secure file manager or SFTP, and confirm you are working in the correct WordPress installation.

Compare the configuration values with the database details shown in the hosting panel. If the provider recently changed a password, use its instructions to confirm the current database password and permissions. Do not guess, and do not make multiple changes at once. A typo can extend the outage or expose credentials.

Check What to confirm Risk to avoid Database name and user They match the values assigned in the hosting account. Editing the wrong WordPress installation or database. Password It is current and entered exactly as provided. Sharing the password in an insecure message. Database host It matches the host's documented value. Replacing it with a guessed hostname. Database permissions The database user can access the intended database. Granting broad privileges without understanding the impact.

Fix label: Correct a confirmed credential mismatch

What changed: If a verified mismatch is found, update only the incorrect database setting in wp-config.php, using the hosting provider's confirmed value. Save the file, then test the site once in a private browser window.

How to roll back: Restore the backup copy of wp-config.php if the change makes the site worse or does not match the provider's confirmed details. Keep the backup private and delete it securely when it is no longer needed.

Check Database Health, but Do Not Rush Into Repair

Some hosting dashboards offer a database status check or repair option. A database may need repair, but a connection error alone is not enough reason to run a repair command. First confirm that the database server is available and that the connection settings are correct. If the database contains current contact submissions or other business records, make a database backup before attempting a repair.

Use a repair tool only when you understand what it changes and have a usable backup. If you are unsure, ask the host to inspect the database and explain whether a repair is recommended. Do not delete tables, recreate the database, or restore an old backup as a first step. Those actions can cause permanent data loss or remove recent leads.

Restore the Site and Protect Leads

After a change, verify more than the homepage. Check key practice-area pages, the contact page, mobile display, and the firm's approved contact information. If a form appears to be working again, submit a controlled test using a designated internal address and confirm that the test is received. Do not use a real client's information for testing.

Ask the person responsible for the site or hosting to check whether submissions made during the outage were stored. Some forms save entries in WordPress; others only send email, and some do both. Do not assume that a form submission was received just because a visitor saw a confirmation message. Follow the firm's normal process for handling inquiries and any applicable confidentiality or retention requirements.

If the site remains down, keep the maintenance message visible through an available approved channel and keep the alternate phone route easy to find. If a cached version of the site remains visible, it may display an outdated contact number, so verify any public notice against the firm's current approved details.

Keep a Clear Record of Each Action

Change one thing <https://fantasticlawyers.com/2026/10/11/best-criminal-lawyers-brisbane/> at a time and record the result. A small incident log helps prevent repeated work and makes it easier to roll back a change or brief another staff member.

Time Action or observation Result Rollback or next step [Time and time zone] Checked hosting status page [Finding] [Next step] [Time and time zone] Compared database settings with provider details [Finding] [Backup location or rollback] [Time and time zone] Tested contact page and internal form submission [Finding] [Follow-up]

What Not to Do During the Outage

- Do not edit database credentials based on guesses.
- Do not restore a backup until you know what data it will replace and have preserved the current state.
- Do not install random plugins or make unrelated WordPress updates during the incident.
- Do not publish database credentials, client details, or private logs in a public forum.
- Do not declare the contact form fixed until a controlled test confirms delivery or storage.
- Do not leave a maintenance message that asks visitors to send confidential legal details through an unapproved channel.

After Service Returns

Once the site is stable, save the incident notes and confirm that backups are current and restorable. Review recent changes, such as password rotations, migrations, or updates, to identify what may have triggered the failure. Make sure the correct staff members know where the approved maintenance message and alternate contact details are kept.

Finally, monitor the site and contact-form delivery for a short period. If the connection error returns, record the exact message and time again; a recurring outage may point to database resource limits, a failing service, or a configuration issue that needs a lasting fix.

First-Response Checklist

1. Confirm the error from another device or network and record the exact message and time.
2. Check the hosting dashboard and service-status page for database or server incidents.
3. Publish a verified maintenance message and alternate contact route if available.
4. Back up wp-config.php before inspecting or editing it.
5. Compare database name, user, password, and host with confirmed provider details.
6. Test important pages and the contact form after service returns.
7. Keep an incident log and confirm whether submissions from the outage period were received.

The safest first response is orderly: document the error, check hosting health, protect the configuration and database, and make sure potential clients can still reach the firm. That approach helps restore contact forms without turning a temporary interruption into a larger security or data-loss incident.