Securing a WordPress site: the checks, and how often.

For a small business owner with an admin login to a WordPress site. The checks that stop most break-ins, where each setting lives, and how to tell it is done.

General guidance, from WordPress.org's own documentation as it read in October 2026. Prices named here are Adam Roe's own as of October 2026.

EVERYTHING UP TO DATE

- [ ] **Dashboard, Updates says you have the latest WordPress**
  Small security releases apply themselves on most hosts. The bigger releases wait for somebody to click Update Now.
- [ ] **No plugin on the Plugins screen shows a new version waiting**
  Plugins are where most of the risk sits. Once a fix is out, the details of the hole are public.
- [ ] **Auto-updates are on for well-known plugins, or updates are tried on a copy first**
  The Automatic updates column on the Plugins screen. On a site that takes bookings or payments, try updates on a copy first.
- [ ] **Every plugin you are not using has been deleted, not just deactivated**
  A deactivated plugin is still on the server. WordPress.org says to delete what you are not using.
- [ ] **Appearance, Themes holds your active theme and not much else**
  Site Health suggests removing inactive themes you are not planning to use.
- [ ] **The PHP version is one that still gets security fixes**
  Tools, Site Health, Info, Server shows it. Try a change on a copy first, because an old plugin may not come with you.

WHO CAN LOG IN

- [ ] **Every name in Users, All Users is somebody you could ring today**
  An old developer's administrator account is one of the easiest ways in there is.
- [ ] **Administrator only for the one or two people who need it**
  Everybody who only changes the words gets Editor or below.
- [ ] **One account per person, and nobody called admin**
  A shared login cannot be taken off one person. WordPress.org says names like admin are tried first.
- [ ] **Two-factor is on for every administrator**
  WordPress does not include it. The free Two Factor plugin from WordPress.org adds it under Users, Your Profile.
- [ ] **Application Passwords you do not recognise have been revoked**
  On the profile page. They let other apps connect, and removing one does not change anybody's password.

A WAY BACK

- [ ] **A backup is taken every day, automatically**
  By the host or a backup plugin. A backup that depends on somebody remembering does not happen.
- [ ] **Backups are kept off the server**
  A backup on the same server as the site goes down with it.
- [ ] **There are a few weeks of them, not one**
  A break-in is often noticed days later. You need a copy from before it, not from last night.
- [ ] **One has been restored onto a copy and opened**
  The only way to know a backup has the database and the uploads in it.

IN FRONT OF THE SITE, AND IN ITS SETTINGS

- [ ] **There is a firewall in front of the site**
  Ask the host. WordPress.org prefers one at the host or in front, so bad traffic is stopped before it reaches the server.
- [ ] **Repeated login attempts are limited**
  The login page is tried by bots all day. The host, a service in front, or a plugin as second best.
- [ ] **The file editor is switched off**
  One line in wp-config.php sets DISALLOW_FILE_EDIT to true. Copy it from the article rather than this PDF, so the quotes stay straight.
- [ ] **Settings, General: both addresses start https://**
  WordPress Address and Site Address. Then check the padlock on every page, the login page included.

IF YOU WANT IT DONE FOR YOU

- [ ] **Hosting, £50 a month**
  Firewall, malware scanning, a daily backup, monitoring, monthly updates checked afterwards, and the site put back if one breaks it.
- [ ] **WordPress maintenance, Manage £300 a month, or £350 with hosting**
  Updates on a staging copy first, a backup restored to prove it, PHP kept current, and who can log in reviewed monthly.
- [ ] **A take-on check, £200, for a site somebody else built**
  Half a day: what it runs on, what is out of date, and who still has access, in writing.

Do the first two sections today. The rest are habits, and they take minutes once the setup is done. **adamroe.co.uk/blog/how-secure-wordpress-site**