Hardening your web server

Better safe than sorry

Change SSH port

Don’t use the default port 22!

Disable root login

Create your own account and grant yourself root-level permissions

Restrict logins per IP address

If possible, only log in from your own static IP address. Or, at least, add a secondary level of protection for unrecognized IPs.

Install mod_security

Open source web application firewall
https://www.modsecurity.org/

Install fail2ban

Fail2ban scans log files and bans IPs that show the malicious signs
http://www.fail2ban.org/

Install brute force protection

(server level and/or application level)

Install 2-Factor Authentication

Use strong passwords

Minimum 11 chars alphanumeric, or "correct horse battery staple” style

https://xkcd.com/936/

Set file permissions to minimum viable levels

chmod 777 is not your friend

Don't use plain FTP

Always use SFTP or SSH

Use SSL on your site

Restrict database permissions

Use a web application firewall

CloudFlare, Sucuri Firewall

Disallow arbitrary code execution

Disallow file editing via your CMS

Stay up to date

Operating system, web server, scripting language, database server.
Core CMS updates, plugins, etc.

Backups!

Keep at least 30 days of rolling backups