ZEYTECH
TECHNOLOGY SOLUTIONS FOR BUSINESS PROBLEMS

108 Packerland Dr Ste D
Green Bay, WI 54303

888-466-8350
`

info@zeytech.com
www.zeytech.com

Website Security Blueprint

Step 1: Foundation Check (Set It and Don’t Forget It)

- SSL Certificate is installed and valid
- All plugins, themes, and CMS are fully updated
- Web Application Firewall (WAF) is active (e.g., Cloudflare, Sucuri)
- Admin panel login uses MFA (multi-factor authentication)
- Old users and plugins have been reviewed and removed

Step 2: Active Protection (Things You Must Monitor)

- Automated daily backups stored offsite
- Uptime and malware monitoring tools are in place
- Email phishing simulation done quarterly with your team
- Password manager in use for all staff logins
- Internal device antivirus + OS updates enforced

Step 3: Audit & Recovery Readiness

- Quarterly security audit (internal or with your MSP)
- Incident response plan documented (who does what if hacked?)
- Access controls reviewed (least privilege principle)
- Cyber insurance coverage reviewed and aligned with risk
- Compliance needs (HIPAA, PCI, etc.) are identified and addressed

Bonus Tools:

- Free Site Scanner: https://sucuri.net or https://securityheaders.com
- Backup Platform: JetBackup, UpdraftPlus, or CodeGuard
- WAF Options: Cloudflare Pro or Sucuri Firewall
- Password Manager: 1Password, Bitwarden

Need Help?
Book a 1-on-1 strategy session at **https://www.zeytech.com/contact**