WordPress Security Checklist

We know that you care about what you build and protecting it is incredibly important. Hacks happen, and it's your job to reduce their likelihood to the lowest probability possible. We built this checklist of best practices to help you harden your website and protect you and your users from hacks.

HOSTING

- ☐ Ideally on a dedicated instance or server
- ☐ For shared hosting, ensure that sites are isolated or "jailed"
- ☐ Run an https-only website

USER MANAGEMENT

- ☐ Grant only as much access as is needed
- ☐ Review your user list frequently, deleting those that are obsolete, downgrading roles where possible

WORDPRESS CORE, THEMES AND PLUGINS

- ☐ Enable auto-updates wherever possible / practical
- ☐ Check for updates frequently (at least weekly) and install them as soon as possible.
- ☐ Only download themes and plugins from trusted sources
- ☐ Remove all unused themes, plugins and old unused WordPress installations immediately

AUTHENTICATION

- ☐ Ideally use 2-factor authentication
- ☐ Require strong passwords for all users
- ☐ Ensure that your login page is running on an https page
- ☐ Limit the rate of login attempts

SERVER ADMINISTRATION

- ☐ Only communicate with your server using an encrypted connection (sFTP for file transfer or SSH for shell access)
- ☐ If you connect to your server over a public network, use a VPN

SERVER ADMINISTRATION (CONTINUED)

- [ ] Secure access to your wp-config.php file, including copies
- [ ] Secure access to your backups, log files, test files, temporary files and other PHP applications on your web server
- [ ] Backup your WordPress files and database at least weekly
- [ ] Use a strong password for your MySQL database user
- [ ] Install a WordPress security plugin like Wordfence

FEATURES TO LOOK FOR IN A WORDPRESS SECURITY PLUGIN

- [ ] Malware scanning
- [ ] Brute-force login protection
- [ ] Protection against hacker recon techniques
- [ ] A WAF with regular rule-set updates
- [ ] Rate based throttling and blocking
- [ ] Two-factor authentication
- [ ] Password auditing
- [ ] Country blocking
- [ ] Advanced blocking techniques

SECURE YOUR WORK ENVIRONMENT

- [ ] Protect your internet connection by using a VPN, especially on public networks
- [ ] Only install trusted software on your workstation and mobile device
- [ ] Use a reputable virus scanner
- [ ] Protect your devices with strong passwords
- [ ] Watch out for phishing, spear phishing and social engineering attacks

TAKE STEPS TO DETECT HACKS EARLY

- [ ] Visit your site often
- [ ] Search for your website in Google frequently
- [ ] Set up email alerts in Google Search Console
- [ ] Use a malware scanner and set up email alerts
- [ ] Investigate customer reports immediately
- [ ] Use a source code scanner to verify site integrity
- [ ] Use a website monitoring service that detects site changes
- [ ] Watch for unexplained spikes in site traffic