Is Your Business Hack-Proof? Find out today!

Cybersecurity doesn't have to be complicated — but it *does* have to be done. This quick self-assessment will help you uncover hidden risks and show you exactly where to strengthen your defenses.

Check off each item you've completed. Unchecked boxes = your action plan for stronger security.

---

1. Website Security

□ Is your WordPress core updated to the latest version?
□ Are all plugins and themes updated regularly?
□ Do you avoid using free or unsupported plugins?
□ Is your website hosted by a security-focused provider (not discount hosting)?
□ Do you have daily backups set up — and tested?
□ Are strong, unique passwords enforced for all users?
□ Is Two-Factor Authentication (2FA) enabled on your WordPress admin?
□ Does your website have a valid SSL certificate (https://)?
□ Is your SSL certificate set to auto-renew?

Why It Matters:

- Keeping WordPress and plugins updated protects you from known vulnerabilities.
- Using trusted hosting providers ensures professional-level security practices.
- SSL certificates encrypt sensitive customer information, protecting data and building trust.
- Regular backups give you a fast path to recovery if something goes wrong.

---

2. Email and Account Security

□ Are you using a professional password manager (like 1Password)?
□ Is 2FA enabled on all key accounts (email, CRM, hosting, etc.)?
□ Do you regularly check for breaches using services like "Have I Been Pwned"?
□ Are employees or partners trained on recognizing phishing attempts?

□ Do you regularly review and remove old or unused user accounts?
□ Are users assigned only the permissions they *absolutely need*?

Why It Matters:

- Email breaches are often the first step attackers take.
- Strong passwords and 2FA block easy access to sensitive systems.
- Regularly auditing accounts reduces the number of ways hackers can sneak in.
- Teaching your team how to spot phishing emails builds a human firewall.

---

3. General Cyber Hygiene

□ Do you always use a VPN when on public or unsecured WiFi?
□ Are brand mentions and business reputation monitored with alerts?
□ Are your devices (laptops, phones) protected by strong passwords or biometrics?
□ Are operating systems and antivirus software kept up to date automatically?
□ Are logins and devices *never* shared between employees or family members?
□ Are backups tested and stored offsite as well?

Why It Matters:

- A VPN protects your data when you're on WiFi networks you don't control.
- Brand monitoring helps you catch impersonation or fake accounts early.
- Keeping devices updated ensures you're shielded from known threats.
- Secure, personal-only devices close off easy paths for hackers.

---

4. Emergency Readiness and Integrations

□ Do you have a simple incident response plan if your site or email gets compromised?
□ Have you audited connected services (payment gateways, forms, CRMs) to ensure they are secure and still needed?

Why It Matters:

- A plan reduces panic in the event of a security incident and speeds up recovery.
- Reducing unnecessary third-party integrations limits possible points of failure and attack.

---

5. Scoring and Next Steps

Scoring Guide:

- 17–21 "Yes" answers: You’re in strong shape — keep it up!
- 12–16 "Yes" answers: You’re doing well but have some important gaps to address.
- 11 or fewer "Yes" answers: It's time to prioritize your cybersecurity immediately.

🎯 Ready to lock down your business?

Book a free 30-minute Cyber-Security Strategy Session at privatenode.io — and move forward with peace of mind.