The Layman's Guide to Securing Your WordPress Website

→ Actionable Steps for Proactive & Reactive Security

Shivanand Sharma
Agenda

1. Importance of Web-Security
2. Why & How Websites Are Hacked
3. Understanding Security Plugins and Their Functions
4. Developing a Proactive Security Framework
5. Strategies for Managing and Securing Compromised Websites
6. Summary
Business: Leveraging Importance of Web-Security

1. Escalating Relevance & Necessity of Cyber-Security

2. Upping Your Game
   a. Niche out: Market Competitiveness
   b. Adopt a Holistic Approach to Envision a Broader Scope for Projects.
   c. Amplify Your Value-Proposition to Clients.

3. Mitigating Risks & Consequences
   a. Immediate Effects: Downtime, Data Breaches, Negative SEO Impacts.
   b. Mid-Term Fallout: Blacklisting & Reputational Impact.
Why Are Websites Hacked: Primary Motivations

1. **SEO Manipulation**
   — Higher Traffic - Higher Reward by Redirecting traffic.

2. **Geopolitical Conflict and Cyber-Revenge**
   — Leading to Website Defacement.

3. **Cryptocurrency Mining**
   — Cryptojacking Hogs CPU, Memory and Other Resources of the Server as Well as the Client (Browser).

4. **Data-Theft**
   — Data-Theft, Ransomware, or Using Compromised Sites as Part of Larger Botnets.
Anatomy of an Attack: The Request-Response Chain

1. **Incoming Request**
   — Initiated by the Client; Travels Through the Network.

2. **Passes Through Proxies / Firewalls**
   — Transits across various network nodes and proxies.
   — Filtered Through Various Firewalls \[ Allowed \| Denied \] (System, Router, ISP, CDN / WAF).
     - **Vulnerabilities Due to** Insufficient Firewall Measures and Lack of Hardening.
       a. **DDoS & Brute-Force Attacks** From Inadequate Protection.
       b. **Software Vulnerability Exploitation / Malware-Infection**.

3. **Server Processes Request**
   — Renders HTML (or JSON) Etc.

4. **Server Sends a Response**
   — Contains Headers & Body.
Security Plugins Simplified

1. Vulnerability Scanning
   — Anticipating Threats
2. Firewall Protection
   — The First Line of Defense
3. Hardening
   — Hardening the Website Against Common Threats
4. Malware Remediation
   — Detect & Disinfect
Security is not a plugin; it is a mindset.

Embrace Security as a Culture, Not Just a Code.
Blueprint for Proactive Security

1. **Access Management**
   Continuously Revise Access in Line With Role Changes and Responsibilities.

2. **Backups**
   Essential for Recovery, Regardless of Infection Status.

3. **SSL**
   Secures Data in Transit From MITM Attacks; Isn’t a Comprehensive Security Solution.

4. **Website Hardening & Protection**
   First Level of Defense; Protects Website From Rogue Traffic, Resource hog, Pentesting, DDoS.

5. **Regular Updates** — Major, Minor vs. Patch, Maintenance & Security
   Do Not Indiscriminately Block WordPress Updates.

6. **Periodic Review & Audit**
   Maintain Vigilance and Proactivity in Security Measures.
Reactive Security: Symptoms of a Hacked Website

1. **Redirects**
   — Unexpected Website Redirects

2. **Performance Issues**
   — Slow Website / Frozen Browser

3. **Spam**
   — Spam Web Pages / Defaced Design

4. **SEO**
   — Sudden Drop in Search Results
   — Cryptic / Garbled Text in SERPS

5. **Blacklisting**
   — Alerts From GSC, Etc.
   — Ad-Campaign Suspension
   — Outgoing Emails Marked as Spam

6. **Access**
   — Unauthorized User Accounts
Reactive Security: Securing a Compromised Site

Triage Management — CURE

1. **Check**
   — Confirm the Breach and Assess Its Scope.

2. **Undertake**
   — Put Website Into Maintenance to Avoid Spread, Impact to Visitors & SEO.
   — Implement Immediate Protective Measures and Utilize Necessary Tools.

3. **Remediate**
   — Conduct Thorough Scans, Clean Up and Reinforce Security.

4. **Evaluate**
   — Attack-Attempts Are Frequent Immediately After a Cleanup.
   — Continuously Monitor for Any Further Anomalies or Issues.
Common Everyday Mistakes

1. **Not Verifying Your Backups**
   — Test restoring a backup to a sandbox to ensure that backups can be restored in case of any eventuality.

2. **Restoring Backups Prematurely**
   — Risk of Reintroducing Vulnerabilities or Backdoors Leading to Repeated Malware Infections.

3. **Blocking Security Updates**
   — Essential for Addressing and Patching Vulnerabilities.

4. **Installing Unverified Themes and Plugins**
   — Potential Sources of Rogue Code and Backdoor Access.

5. **Multiple Security Plugins**
   — Hit & Trial Hoping Something Would Work

6. **Starting Fresh**
   — Cleaning Websites is Simpler
Summary: Key Takeaways for Robust Web Security

1. **Value-Driven Niche Strategy**: Elevate your offerings for enhanced business prospects.
2. **Universal Vulnerability**: Every site is at risk, targeted for profit, not personal reasons.
3. **Informed Use** of Security Plugins: Understand their roles to prevent overreliance.
4. **Cultivating a Security Mindset**: Security transcends tools; it's an integral part of organizational culture.
5. **Team Awareness and Education**: Regularly update your team on security best practices and internal procedures.
6. **Establish Security Protocols**:
   a. Efficient access management.
   b. Consistent security checks.
   c. Routine audits.
   d. Effective Triage Management.
Q&A — Vote of Thanks — Stay Connected

https://www.youtube.com/@malcure
https://twitter.com/CyberMalcure
https://www.linkedin.com/company/malcure/
https://www.facebook.com/malcurewebsec
https://malcure.com