Malware Infection Audit Checklist

20-Point Website Malware Recovery Audit

☐ Have all WordPress users been reviewed?
☐ Have all passwords been rotated?
☐ Has hosting/FTP access been changed?
☐ Have suspicious PHP files been scanned?
☐ Have modified plugin files been reviewed?
☐ Has functions.php been inspected?
☐ Has uploads folder been checked for executables?
☐ Has the database been searched for injected code?
☐ Have rogue redirects been removed?
☐ Have cron jobs been inspected?
☐ Have inactive plugins/themes been deleted?
☐ Have file permissions been reviewed?
☐ Has a malware scanner been installed?
☐ Have file integrity alerts been enabled?
☐ Has Search Console security status been checked?
☐ Have spam URLs been reviewed?
☐ Has blacklist review been requested if needed?
☐ Are backups verified clean?
☐ Is MFA now enabled?
☐ Is monthly malware review scheduled?

Scoring:

17–20 = Strong malware recovery maturity
12–16 = Residual exposure remains
0–11 = High reinfection probability