Compromised Website Recovery Guide

Immediate steps to contain, clean and safely restore a hacked website.

Important
If customer data, payment data or credentials may have been exposed, follow your legal, contractual and incident-response obligations in addition to technical cleanup.

1. Contain the Incident

- If the site is actively serving malware or phishing, restrict public access while you investigate.
- Preserve logs and a copy of the compromised files for analysis.
- Do not delete evidence before you understand how the compromise occurred.

2. Change Credentials

- Change Client Area, Plesk, FTP/SFTP, SSH, database and application administrator passwords.
- Revoke old API keys and application passwords where applicable.
- Enable two-factor authentication on important accounts.

3. Identify the Entry Point

- Review recently modified files and application logs.
- Check for outdated plugins, themes, CMS versions or leaked credentials.
- Look for unexpected admin users, scheduled tasks and malicious PHP files.
- Do not simply remove visible malware without fixing the underlying weakness.

4. Restore or Clean

- Prefer restoring a known-clean backup when available.
- If cleaning manually, replace core application files with verified originals.
- Remove malicious files and unauthorized users.
- Patch the vulnerability before reopening the site.

5. Validate

- Scan again after cleanup.
- Check DNS, redirects, cron jobs and mail sending.
- Monitor logs closely after the site returns online.
- Keep a clean recovery point once the incident is resolved.

Recovery Checklist

✓ Site contained

✓ Logs preserved
✓ Passwords rotated
✓ Entry point identified
✓ Malware removed
✓ Software patched
✓ Site rescanned
✓ Monitoring enabled