Hack recovery checklist

After a WordPress hack: contain it, keep evidence, find the way in, clean, harden, recover.

Check off each item as you go. Keep a printed copy somewhere other than your computer.

CONTAIN IT

- [ ] Work from a device you trust is clean.
- [ ] Turn on maintenance mode or block public access at the host or firewall.
- [ ] Change hosting, SFTP/SSH, email and WordPress admin passwords. Remove unknown SSH keys.
- [ ] Change the database password and update DB_PASSWORD in wp-config.php to match.

KEEP EVIDENCE FIRST

- [ ] Download the files and database as they are. Label the copy infected and store it apart.
- [ ] Save access and error logs before they rotate, and ask your host for theirs.
- [ ] Keep a timeline of what you saw and every change you make.

FIND THE WAY IN

- [ ] Search access logs for POSTs to odd PHP files, wp-login.php and xmlrpc.php near the start.
- [ ] List changed PHP files: find . -name "*.php" -mtime -14. Widen the window as needed.
- [ ] Uploads should hold no PHP: find wp-content/uploads -name "*.php".
- [ ] Run wp user list --role=administrator and note any admin you did not create.
- [ ] Check wp option get siteurl and home, and wp cron event list for odd hooks.
- [ ] Inspect .htaccess, wp-config.php, index.php and wp-content/mu-plugins for injected code.
- [ ] Note outdated plugins: wp plugin list --update=available. One is often the way in.

CLEAN IT

- [ ] Restore a backup from before the break-in if you have one, then patch the hole.
- [ ] Otherwise run wp core download --force --skip-content, then wp core verify-checksums.
- [ ] Reinstall plugins and themes from the source, then wp plugin verify-checksums --all.
- [ ] Delete what you cannot trace to a source: plugins, files, mu-plugins, admin users.
- [ ] Search the database for injected code: wp db search "<script" and "base64_decode".

HARDEN AND RECOVER

- [ ] Require 2FA for every admin, and downgrade accounts that do not need admin.
- [ ] Replace the salts in wp-config.php with new keys from api.wordpress.org/secret-key/1.1/salt/.
- [ ] Update everything, delete unused plugins and themes, and set DISALLOW_FILE_EDIT to true.
- [ ] Check the Search Console Security Issues report and request a review once clean.
- [ ] Check Google Safe Browsing status, and email blocklists if the server sent spam.
- [ ] If personal data may be exposed, check your notification obligations with a lawyer.
- [ ] Watch logs and file changes for 30 days. Reinfection often means a missed backdoor.