How to prevent a hack: a security checklist for small business websites

- [ ] **Regular updates** You can do this yourself
  Updating the WordPress core, the theme and the plugins is the most important protection.
- [ ] **Backups stored independently of your hosting** Worth leaving to an expert
  If your hosting account is hacked, or the host suspends it, the backups stored on it may be out of reach too.
- [ ] **Two-factor authentication** You can do this yourself
  Turn it on for WordPress administrator accounts, your hosting, your domain manager and every connected service (for example Google Tag Manager, Shopify staff accounts).
- [ ] **Unique, strong passwords** You can do this yourself
  Every service needs a different password, stored in a password manager.
- [ ] **Regular review of access** You can do this yourself
  Every quarter, check who has access to the site, the hosting and the connected accounts.
- [ ] **Licensed plugins and themes only** Leave the check to an expert
  Never use a cracked ("nulled") premium theme or plugin downloaded for free: they almost always contain a hidden back door.
- [ ] **Delete unnecessary plugins and themes** You can do this yourself
  A deactivated plugin still stays on the server, and if it is vulnerable, it can still be attacked.
- [ ] **Firewall and hardening** Worth leaving to an expert
  A web application firewall (WAF) filters out known attack patterns, while correct file permissions and a few WordPress settings (for example disabling the file editor in the admin) make the attacker's job harder.
- [ ] **An up-to-date PHP version** Worth leaving to an expert
  The PHP version running on your hosting also has a support period.
- [ ] **One site, one hosting account** Discuss it with your host or developer
  If several sites run on one hosting account, one hacked site can infect the others.
- [ ] **Google Search Console** You can do this yourself
  Register your site and check that notifications go to your email address.
- [ ] **Uptime monitoring** You can set it up yourself
  An uptime monitoring service checks your site every minute and tells you when it goes down.

A 15-MINUTE MONTHLY ROUTINE

- [ ] Check for pending updates.
- [ ] Check that the latest backup was completed.
- [ ] Go through the user list.
- [ ] Type site:yourdomain.com into Google and look for foreign results.
- [ ] Look at the Search Console notifications.

The full article with explanations: https://redwebdesign.hu/en/knowledge-base/website-security-checklist/

Ferenc Kulcsár · hello@redwebdesign.hu · +36 30 501 9090